University of Southampton

Faculty of Engineering and Physical Sciences
School of Electronics and Computer Science

A pedagogical design model to create serious games for cyber security

by

Stephen James Hart

MSc BSc (Hons) CISSP CISM CCSP

ORCiD: 0000-0001-5108-7116

A thesis for the degree of
Doctor of Philosophy

May, 2022

University of Southampton

Abstract

Faculty of Engineering and Physical Sciences
School of Electronics and Computer Science

Doctor of Philosophy

by Stephen James Hart

Cyber attacks have been increasing, and there have been many media reports of attacks against large and small organisations, causing financial loss and reputational damage. Organisations invest in professional training courses for their employees to raise awareness of cyber attacks and related defences. However, traditional approaches have failed to effectively educate employees, as testified by the increasing number of successful cyber attacks exploiting human factors. Serious games are an effective alternative tool to educate and train people on cyber security concepts. There is consensus on the benefits and potential of creating serious games and gamification techniques, which applies game mechanics to non-gaming activities, such as training to make the exercise more engaging. Many serious games have been created without a transparent and formal design process. There are currently several pedagogical models, frameworks, and methodologies for designing and analysing serious games that provide valuable interpretations. None of the models is designed specifically for serious cyber games, and these models focus primarily on high-level aspects and requirements. Many design models fail to address higher-order thinking skills and do not consider the target players' different needs. They do not help understand how such high-level requirements can be concretely satisfied and not a detailed explanation of how to design a serious game in a step-by-step process.

This thesis proposes a new pedagogical model called MOTENS to design serious cyber games for awareness and education. The MOTENS model was developed from the experience of creating Riskio, a multiplayer tabletop game to increase cyber security awareness for people with a technical and non-technical background working in organisations and university students. A new serious game called CIST: A serious single-player online game for hardware security supply chain was designed using the MOTENS model. The CIST game was then tested to verify that the game mechanics design selected using the MOTENS model achieved the desired learning outcomes. The CIST game was played and evaluated in a workshop on hardware security threats and defences for MSc/PhD students. Some issues reported by the students were identified as failure of the CIST game design and not the MOTENS model. As with the Riskio game, the CIST game proved popular with the target players and increased players participation in learning. Further research is required to develop the MOTENS model by creating and designing/evaluating different types of serious cyber games.

Contents

List of Figures

List of Tables

List of Terms and Acronyms

APT Advanced Persistent Threat.

ARG Alternative Reality Game.

ATMSG Activity Theory-based Model of Serious Games.

Behavioural In marketing, behavioural segmentation is the process of dividing a broad consumer or business market.

BEOL back-end-of-line.

CCSP Certified Cloud Security Professional.

CEH Certified Ethical Hacker.

CIA Confidentiality, Integrity and Availability.

CIS Center Internet Security.

CISM Certified Information Security Manager.

CISSP Certified Information Systems Security Professional.

CIST Counterfeiting, Information Leakage, Sabotage, Tampering.

CLE Constructivist Learning Environments.

CRP challenge–response pair.

CSA Cyber Security Academy.

DDoS Distributed Denial-of-Service.

Demographic The statistical study of populations, defined by criteria such as education, nationality, religion etc.

DREAD Damage potential, Reproducibility, Exploitability, Affected Users, and Discoverability.

EMEA Europe, the Middle East and Africa.

EoP Elevation of Privilege.

ERGO Ethics and Research Governance Online.

EU European Union.

FEOL front-end-of-line.

GDPR General Data Protection Regulation.

GOM Game Object Model.

IATED Int Assoc Technology Education & Development.

IC Integrated Circuit or Chip.

IDS Intrusion Detection System.

IEC International Electrotechnical Commission.

IQR Interquartile Range.

ISMS Information Security Management System.

ISO/IEC International Organization for Standardization/International Electrotechnical Commission.

ITU Intention to Use.

Likert scale The Likert rating scale is a type of psychometric survey scale. The question has a series of answers to choose from, ranging from one extreme attitude to another, generally with a moderate or neutral option.

LINDDUN Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of information, Unawareness, Non-Compliance.

NCSC National Cyber Security Centre.

Netlist is a description of the connectivity of an electronic circuit.

NIST National Institute of Standards and Technology.

OWASP The Open Web Application Security Project.

PDQ Process Data Quickly.

PEOU Perceived Ease of Use.

PKI Public Key Infrastructure.

Psychographic The study of consumers based on their activities, interests, and opinions. It goes beyond classifying people based on general demographic data, such as age, gender, or race. Psychographics seeks to understand the cognitive factors that drive consumer behaviours.

PU Perceived Usefulness.

PUF physical unclonable function.

RPG Role Play Game.

RTL register-transfer level.

Scaffolding Refers to various instructional techniques used to move students progressively toward more robust understanding and, ultimately, greater independence in the learning process.

SDT Self-Determination Theory.

SGDAF Serious Game Design Assessment Framework.

SMEs small-medium enterprises.

SoC system on a chip.

STRIDE Spoofing, Tampering, Repudiation, Information Disclosure & Elevation of Privilege.

TAM Technology Acceptance Model.

VPN Virtual Private Network.

Acknowledgements

I want to thank my supervisors, Professor Vladimiro Sassone and Professor Federica Paci, whose support, patience, advice, and assistance have guided me by successfully creating the serious cyber game called Riskio. The next stage of my PhD is thanks to Professor Sassone and Dr Halak for the help and support in creating the MOTENS cyber serious games design model and the CIST serious game. Special thanks to Dr Halak, who managed to organise a hardware security workshop to test the CIST game during Covid-19 pandemic restrictions. I know this has taken much work to organise at Southampton University. The other experiments at Southampton University and China organised by Professor's Sassone and Paci for the Riskio game were a key component of my research. I would also like to thank all the participants for playing my games and completing the surveys, interviews and experiments. I would also like to thank Dr Gary Wills, who encouraged me to apply to Professor Sassone for my PhD after completing my MSc in Cyber Security.

Thanks to Professor Sassone for organising the weekly Wednesday Microsoft Teams calls during the Covid-19 pandemic whilst working from home. These weekly calls with the Cyber Security Research Group kept me sane and in contact with my fellow PhD students.

I completed my PhD part-time whilst working full time, and a special thanks to my work colleagues Aklima and Anthony, whose continued moral support kept me focused on my PhD research over the years. They both helped when asked to play my games and verify my attacks and defences in the gameplay.

I want to thank my wife Helen and my son Elliot for their continued support for the four years of my PhD when I spent most evenings, weekends, and most of my holiday working on my PhD. Also, for the six years of previous distance learning to get my BSc and MSc and my year off work to get my second MSc in Cyber Security at Southampton University. Finally, thanks to my mum, who always encouraged me and believed I could do this.

Declaration of Authorship

Title of thesis: **A pedagogical design model to create serious games for cyber security**

I, **Stephen James Hart**, declare that this thesis and the work presented in it is my own and has been generated by me as the result of my own original research. **I confirm that:**

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published work of others, this is always clearly attributed;
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. Parts of this work have been published as:

   Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. Computers & Security, 95, 101827. **https://doi.org/10.1016/j.cose.2020.101827**

   Hart, S., Halak, B., & Sassone, V. (2021). MOTENS: A Pedagogical Design Model for Serious Cyber Games. **https://arxiv.org/abs/2110.11765**
8. Online Links:

   www.riskio.co.uk Riskio Website.

   www.riskio.online Shows how the game is played

   mygame.page/cist-game CIST Game

Signature:.....**Date:** Monday 9th May, 2022
Author: Stephen Hart

Chapter 1

Introduction

1.1 Problem Statement / Motivation

Cyber attacks have exponentially increased in the last decade. Threat actors continuously improve their cyber weapons to timely and effectively exploit vulnerabilities, misconfiguration of IT systems and new technologies such as the Internet of Things and Cloud Computing (Symantec, 2019). Since the cyber security landscape is rapidly changing, organisations must keep pace with emerging threats to be resilient against cyber attacks.

In this context, the management of cyber security risks is a key business objective for every organisation. Several standards and frameworks have been proposed to help organisations manage the cyber risks, for example:

- The Cyber Essentials scheme from the NCSC in the UK (NCSE, 2020)
- The NIST Cyber Security Framework (NIST, 2021a)
- The IEC 62443 Security for industrial automation and control systems (IEC, 2021)
- ISO/IEC 27001 for information security management (ISO/IEC, 2021)
- CIS, Top 18 Critical Security Controls for Effective Cyber Defence (CIS, 2021)

As said by 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."
>
> – Kevin Mitnick (Mitnick and Simon, 2003)

Attack techniques targeting humans, so-called social engineering, have become widely diffused and highly effective for perpetrating cyber attacks. Therefore, it is fundamental for organisations

to ensure that all employees are educated on cyber security concepts and aware of the risks posed by even the most superficial cyber attacks, e.g. phishing emails. Organisations have used tailored training and awareness programs to improve the resilience against cyber attacks of their employees.

Today's organisations' IT infrastructure is constantly changing rapidly to use emerging cloud services, and cyber attacks can disrupt organisations' operations, creating potential financial and reputational damage to an organisation. Neghina and Scarlat (2013) suggest that unless an organisation has developed a cyber-threat risk assessment process, it cannot sustain a good security environment. Senior executives of organisations need to make investment decisions on what, where and how much to spend to prevent a successful cyber attack. Many of the issues presented as part of organisational cyber security training programs are universal but must always address a particular organisation's needs and security policies (Nagarajan et al., 2012). For small-medium enterprises (SMEs), the UK Government Cyber Essentials Scheme (NCSE, 2020) proposes five essential controls. Since 2012, the guidance designed for larger organisations looking to protect themselves in cyberspace was the National Cyber Security Centre (NCSC) *'10 Steps to Cyber Security'*, which most FTSE350 companies have used. The 10 steps guidance is also supported by the paper *'Common Cyber Attacks: Reducing the Impact'*. Industry experts have suggested that implementing the five essential controls could stop 80% of the most common attacks (Continuity and Forum, 2018). However, the limitations of Cyber Essentials are that it was designed for SMEs, does not consider cloud services and does not consider the information asset values. Executives and senior managers of SMEs and larger organisations need to know more than just the five essential controls in Cyber Essentials and have a methodology to identify cyber threats to reduce the risk of a vulnerability being exploited.

Most companies fail to invest in cyber security education, and the majority of awareness campaigns are optional and continual where end-users decide if they want to participate (Korpela, 2015). Gamification and the creation of a serious game could be a way to improve executive participation and employee engagement for them to learn organisation specific vulnerabilities to cyber attacks (Fielder et al., 2016) and possible defences to these attacks. Korpela (2015) proposes the potential benefits of using data analytics to combine existing data sources to provide additional value to training programs. These data sources can help design serious games, such as organisational risks from risk register known to the players in creating the game objectives to make the game relevant. The design is about the balance between serious game objectives and entertainment, and clear goals will help players assimilate the pedagogical aim of the game (Le Compte et al., 2015).

1.2 Pedagogical gaps serious cyber game design

Gamification is maturing as an academic research object, as can be seen in the increased number of papers published, two papers in 1995 and 799 papers in 2017, see Figure 1.1 (Luo, 2021). The

first wave of papers of gamification research was about questions of 'what?' and 'why?', the current wave is asking differentiated questions around 'how?', 'when?', and 'how and when not?' (Nacke and Deterding, 2017). There are currently several pedagogical models, frameworks and methodologies for the design and analysis of serious games that provide useful interpretations (Carvalho et al., 2015). None of the models is designed specifically for serious cyber games, and these models focus mostly on high-level aspects and requirements. They do not help understand how such high-level requirements can be concretely satisfied (Carvalho et al., 2015). All the models found for serious games have a dualist approach that the models are for both designing and analysis of serious games. Many serious games have been created on a whim, without a clear and formal design process (Mora et al., 2015). Several games in academic studies cannot be found in a product search and raise questions on suitability (Hendrix et al., 2016). The lack of accessibility to some serious games and unclear design principles or objectives limits pedagogical models to assess them. Many of the design models fail to address higher-order thinking skills, and games often feel more like gamified quizzes (Savvani and Liapis, 2019). For designing serious games, many models lack the methodology of linking game mechanics back to the learning mechanics or lack a detailed design process for a games designer to follow. Not all the models also considered the impact of the design process on players' engagement learning effects (Savvani and Liapis, 2019).

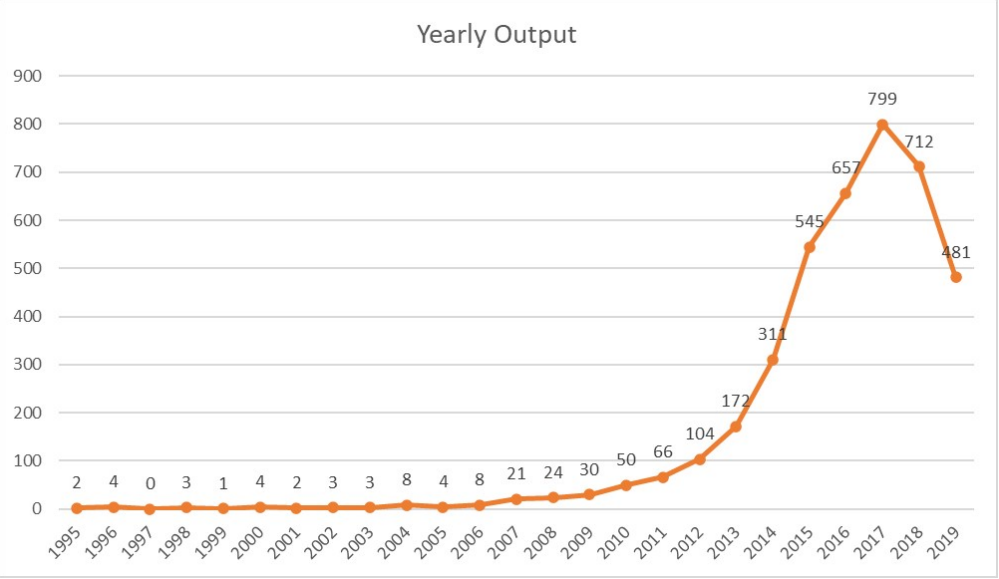


Figure 1.1: Gamification Publication Trends 1995 - 2020 (Luo, 2021).

In summary, no pedagogical design model was found that could be used for the design of serious cyber games that: design does not consider the target players' needs; mapped game mechanics to learning objectives; step by step design process; supported by pedagogical learning theory; or assesses players' higher-order thinking skills. A bias in the models found also used examples for evaluating serious games and not a detailed explanation of how to design a serious game in a step-by-step process.

1.3 Research Aims and Objectives

The purpose of this thesis is: "*Can one using pedagogical design model, create a serious cyber game to teach cyber security awareness and education to meet organisational objectives? The games must be able to be played with technical and non-technical staff with no background in cyber security. Can the games also teach cyber security threats, vulnerabilities and defences and be adapted to organisational specific industry threats and vulnerabilities*". To achieve the presented aim and satisfy the listed requirements, we propose a new serious cyber games design model with the following objectives.

1. The model needs to be used to design serious cyber games for awareness and education. The games should not be restricted to any one type and can be card games, computer-based games, board/tabletop games or speciality games.
2. Must be able to design serious games for different target players, technical, non-technical and from different backgrounds.
3. Serious games must be adaptable to create fictional contexts based on real-world problems.
4. The design model must be adaptable to change the games designed to use different threat models.
5. The model must be able to link the game mechanics to the pedagogical intent.
6. The model must be able to link industry-standard defences as countermeasures to attacks.

1.4 Our Solution

Chapter 7 proposes a new pedagogical design model for serious cyber games for awareness and education called MOTENS. The MOTENS model has improved on current models: 1) they do not link game mechanics to the learning objectives; 2) high-level model and will not assist in the selection of game mechanics to achieve serious game objectives; 3) are mainly assessed in terms of the quality of their content, not in terms of their intention-based design. We feel the improvements in these three areas using the MOTENS model: 1) Can link the game's mechanics to the target players and select the appropriate game's mechanics to meet the learning objectives, supported by pedagogical learning theory; 2) MOTENS has a five-step process to assist in the game design in stage 4; 3) Learning objectives are built into all six components of the MOTENS model and through the five stages in designing serious games.

1.5 Key Contributions

The contributions of this thesis are summarised as below.

Multi-player Serious Tabletop Game. Riskio: A serious game for cyber security awareness and education (see Chapter 4). We created the game to learn and develop the MOTENS serious cyber games design model. Complete information on the game design is published on the website[1] see Figure 1.2.

Riskio Published Paper. The Riskio paper has been published in Elsevier Computers and Security[2]. The Riskio game was designed that the games board and cards can be changed to suit the target players and the desired learning objectives.

Figure 1.2: Riskio Game Website Home Page.

Riskio Game for Sale. The Riskio game is available online provided at cost on request. The Covid-19 pandemic has delayed the printing of the game. Currently, we have over thirty requests for a copy of the games from Universities and commercial organisations in EMEA, Canada, USA. Some of these requests are from organisations wanting to use Riskio to train new graduate intake.

Online Serious Cyber Game. Riskio Online[3] was created during the Covid-19 pandemic to assist games master playing remotely online with up to 4 players.

Serious Cyber Games Design Model. The serious pedagogical games design model is named MOTENS (Figure 7.3) with a detailed model (Figure 7.6). The MOTENS model links the pedagogical theory of learning and the game mechanics to selected games mechanics with five-stage design guidance. In stage 4, the detail five steps for selecting game mechanics (subsection 7.3.1).

Single Player Online Serious Cyber Game. CIST: A Serious Game for hardware supply chain[4] (see Chapter 8) which we created to educate players on the threats and possible countermeasures

[1] www.riskio.co.uk
[2] https://doi.org/10.1016/j.cose.2020.101827
[3] https://riskio.online/
[4] https://mygame.page/cist-game

in the IC hardware supply chain. We created the game using the MOTENS pedagogical design model to demonstrate how to use the MOTENS model to create a serious cyber game for awareness and education.

1.6 Thesis Structure

This thesis is organised into five parts: Part I: Literature Review and Serious Cyber Games. Chapter Two literature review and assessment of serious cyber games. Part II: Create a New Serious Cyber Game. Chapter Three explains the design decisions of the new proposed serious game called Riskio. Chapter Four explains the development of the Riskio game. Chapter Five evaluates the Riskio game and discusses and reflects on pedagogical models for serious games design. Part III: Pedagogical Model to Design Serious Cyber Games. Chapter Six uses what was learned in creating and evaluating Riskio to assess pedagogical models to design serious cyber games. Chapter Seven proposes a new pedagogical model to design serious cyber games called MOTENS. Part IV: Create New Game Using MOTENS, a New Pedagogical Model. Chapter Eight uses the MOTENS model to create a new serious cyber game called CIST to test the efficacy of the MOTENS model in creating a serious game and the evaluation of the CIST game created using the MOTENS model. Part V: Conclusions, Contributions and Future Work. Chapter Nine conclusions, a summary of main contributions of this thesis future work.

Part I

Literature Review and Serious Cyber Games

Chapter 2

Literature Review

This chapter introduces gamification techniques for serious cyber games, a pedagogical approach to serious games design, and methodologies for risk management. The next stage introduces the current cyber games available. It identifies gaps to create a new game whose design is based on a repeatable pedagogical process to meet the research objectives.

2.1 Gamification and Serious Games

Gamification is about applying game mechanics to non-gaming activities, for example, training to make the activity more engaging (Routledge, 2016; Paharia, 2012; Deterding et al., 2011a). Serious games typically provide an immersive in-game environment to play out subject related scenarios (Hill et al., 2020). The term 'Serious Game' is used in this paper to define a game for other than just pure entertainment. Other synonyms used in research papers are 'educational game' or 'learning game' (Roepke and Schroeder, 2019). Serious games use these techniques to provide a fun, enjoyable educational environment where the game participants learn by playing the game. McGonigal (2011) defines four traits of a game: 1) The goal is the specific outcome that players will work to achieve. 2) The rules that place limitations on how players can achieve the goal. 3) The feedback system that tells the players how close they are to achieving the goal. 4) Voluntary participation that requires everyone is playing knowingly and willingly accepts the goal (1), the rules (2) and the feedback (3). The last trait of voluntary participation is essential in players' motivation. Deci and Ryan (2008) proposed a macro-theory called Self-Determination Theory (SDT). However, the work started on SDT in the 1970s. SDT can be applied today to gamification. SDT presents motivation as extrinsic motivation, the external factors, and intrinsic motivation, the internal factors. SDT also presents three basic psychological needs:

- *Competence* - Can perform the activity well
- *Autonomy* - Feeling you are in control
- *Relatedness* - Sense of belonging

One requires all three basic psychological needs to be intrinsically motivated, and for extrinsic motivation, at least competence and relatedness must be satisfied (Conejo et al., 2019). Conejo & Hounsell (Conejo et al., 2019) propose modifying the existing framework to assist designers of games. They propose that some game design frameworks address motivation superficially while others focus exclusively on motivation (Deterding, 2012). Several studies have supported SDT as an approach to work motivation (Gagné and Deci, 2005).

2.2 Pedagogical Game Design

The internet revolution calls for a revamp of curriculum content (Seng Tan*, 2004). The internet as a disruptor requires educators to review the pedagogical approach to curricula to promote high-order thinking skills (Bloom et al., 1956). The revamp is required to deal with the challenges of the internet revolution bringing new threat actors and threats to ensure curriculum content is current and relevant to the learners. Higher-order thinking skills can be considered one of the demanded skills that are highly required, over the requirement for lower-order thinking skills of recalling information, as memorisation is becoming more complex (Qasrawi and BeniAbdelrahman, 2020). Because the information and facts are increasing dramatically, the need to remember the complex nature of cyber attacks defences is insufficient. Therefore, the inclusion of Bloom's higher-order thinking skills to analyse, evaluate and create (see Table 2.1) is even more critical.

The constructivism theory is based on the belief that learning occurs as learners are actively involved in meaning and knowledge construction instead of passively receiving information (Fosnot and Perry, 1996). The constructivist-oriented approach concentrates on the learners constructing their understanding during social interactions (Maor, 1999a). Therefore, using gamification to teach cyber security awareness and education, the game must promote the interactions that increase the discourse and personal construction.

Driscoll (2000) summarised the five conditions for instruction for constructivism are: (1) complex and relevant learning environment; (2) social negotiation; (3) multiple perspectives and multiple modes of learning; (4) ownership in learning; and (5) self-awareness and knowledge construction, see Figure 2.1.

The traditional approach to education does not present problems to students but presents content to resolve problems (Seng Tan*, 2004). Tan(1994) survey with academic staff (n = 65) found that only 27% gave a high rating in considering the 'learner', where content scored 65% (Seng Tan*, 2004).

Three areas are driving the change to problem-based learning. The first is an increasing demand for bridging the gap between theory and the real world. The second is the increase in information and accessibility to the information. The third is an emphasis on solving real-world problems (Seng Tan*, 2004).

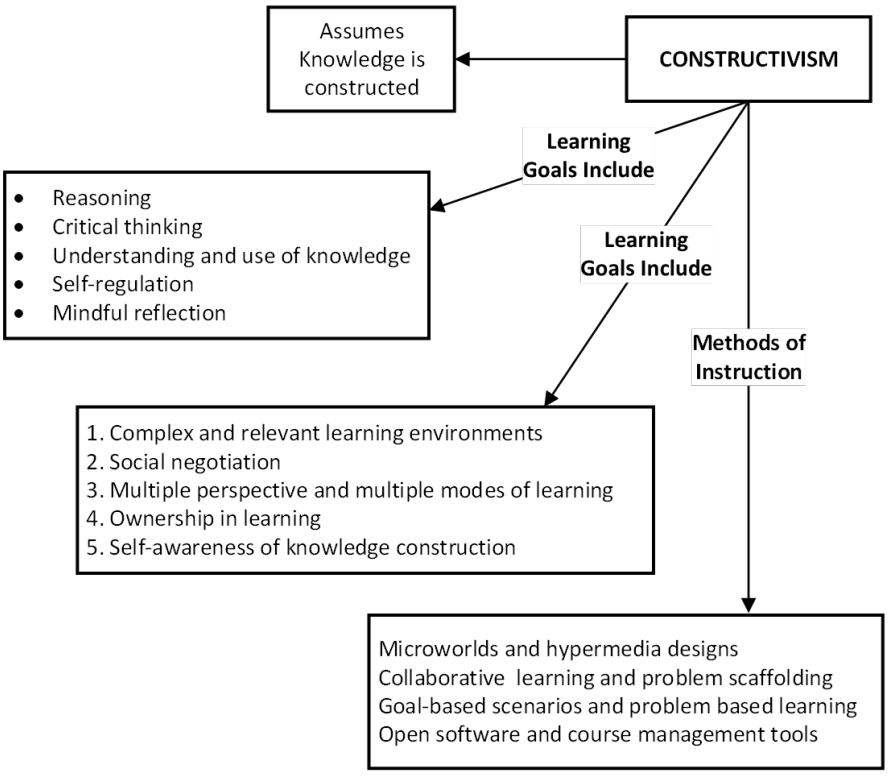


Figure 2.1: Driscoll Constructivism Learning Theory (Driscoll, 2000).

The move to problem-based learning will also require the shift in three loci of educational preoccupation: (1) content coverage to problem engagement; (2) from lecturer to coach; and (3) from passive student learning to problem solvers (Seng, 2000), see Figure 2.2.

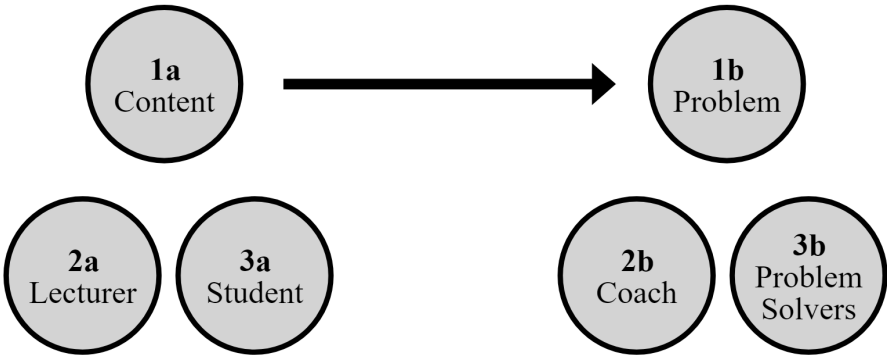


Figure 2.2: Model of Curriculum Shift to Problem Based Learning (Seng, 2000).

Learners will sometimes memorise information without understanding the concept. For example, they may be able to recite what a Distributed Denial-of-Service (DDoS) attack is but not comprehend its meaning, and this would be an example of Bloom's taxonomy of lower-order thinking, see Table 2.1. Gagné has proposed a ***learning hierarchy***, *a set of component skills that must be learned before the complex skill can be learned* (Gagné and Briggs, 1992). Using the DDoS example, learners understand the issues around the 'availability' of systems, understand what a 'distributed attack' is, and understand what a 'denial of service attack' is. Learning these three components should join together to understand a Distributed Denial-of-Service (DDoS).

A player can join components they learn using higher-order thinking skills of evaluation and creation to form new ideas is an example in Bloom's taxonomy of higher-order thinking skills. The opportunities to use higher-order thinking skills can be done through creating fictional simulations. Creating facilitate learning basic lower-order thinking skills (LOTS) and then teaching higher-order thinking skills (HOTS) through replicating the context and aspects of the 'real world' (Charsky, 2010).

Constructivism is not one theory but a multitude of approaches and can seem incommensurable with instructional theory (Driscoll, 2000) but can also be seen as an alternative view.

2.3 Methodologies for Risk Management

There are many recognised standards for risk management, and the two most popular internationally recognised standards are the National Institute of Standards and Technology (NIST) SP800-39 (NIST, 2011) and the ISO 27005 (ISO/IEC, 2018). These are both frameworks to manage information security risks effectively. ISO/IEC 27005 is supported by the ISO/IEC 27000 family of Information Security Management System (ISMS), though there are more than a dozen standards. The ISO management standards are a series of mutually supporting information security standards combined to provide a framework for best-practice information security management.

Finding new risks will be one of the most challenging steps for organisations moving to the cloud to use emerging cloud services. The distributed nature of cloud services brings new threats and needs organisations to consider a new model for risk assessment for cloud computing (Zhang et al., 2010).

Why are cyber games essential? The traditional approach to cyber risk assessments will often focus on vulnerabilities in the network or software systems. A few approaches to elicit requirements will focus on exploiting humans (Beckers and Pape, 2016). Key senior stakeholders who approve budgets must understand the vulnerabilities and threat actors specific to their organisation to manage appropriate controls and risks. The number of cyber attacks that target organisations staff is increasing and designed to exploit human factors (Roy et al., 2010) and not directly the vulnerabilities in the network or software systems.

Table 2.1: Blooms Taxonomy Mapped to LM-GM Model.

Learning Mechanic (LMs)	Thinking Skills	Game Mechanics (GMs)	HOTS to LOTS
• Accountability • Ownership • Planning • Responsibility	CREATING	• Design/Editing • Infinite gameplay • Ownership • Planning • Protégé effect • Status • Strategy/planning • Tiles/grids	**High Order Thinking Skills**
• Assessment • Collaboration • Hypothesis • Incentive • Motivation • Reflect/Discuss	EVALUATING	• Action Points • Assessment • Collaboration • Communal Discovery • Game Turns • Pareto Optimal • Resource Management • Rewards Programme • Urgent Optimisation	
• Analyse • Experimentation • Feedback • Identify • Observation • Shadowing	ANALYSING	• Feedback • Meta-game • Realism	
• Action/Task • Competition • Cooperation • Demonstration • Imitation • Simulation	APPLYING	• Capture/Elimination • Competition • Cooperation • Movement • Progression • Selecting/Collecting • Simulate/Response • Time Pressure	
• Objectify • Participation • Questions and Answers • Tutorial	UNDERSTANDING	• Appointment • Cascading Information • Questions and Answers • Role-play • Tutorial	
• Discover • Explore • Generalisation • Guidance • Instructional • Repetition	RETENTION	• Behavioural Momentum • Cut Scenes/Story • Goods/Information • Pavlovian Interactions • Tokens • Virality	**Low Order Thinking Skills**

2.4 Top Authors & Publications and Games Selection and Testing

The method to find serious cyber games involved searching with keywords, for example, to find serious games: *'serious cyber game' or 'gamification' or 'educational game' or 'learning game' or 'game-based learning'*. When searching, we also look for how serious games are designed or assessed and what pedagogical design models were used. The primary search used was the Web of Science[5]. However, additional searches were completed using the University of Southampton online library and Google Scholar[6]. Searches using the Web of Science used an inbuilt search tool based on publication dates for all searches. We used the topic field (TS) for the keywords, which is based on words in Title, Abstract, Author Keywords, and Keywords Plus®. The searches were completed several times to find new published serious games throughout the research period.

2.4.1 Bibliometric Analysis of Gamification Publications 2016 - 2021

The first stage was to find publications on bibliometric analysis of gamification. The bibliometric publications were used to identify top publications, leading journals, influential scholars in serious cyber games and identify keywords used for searches. The Web of Science was searched with a publication date from 01/01/2016 to 31/12/2021, using the following search term.

Bibliometric analyses Search: *(TS=("bibliometric analyses") OR TS=("bibliometric analysis") OR TS=(bibliometric)) AND (TS=(gamification) OR TS=("game-based learning")).*

The search found 28 results which were further reviewed. The review found the majority of 20 were from one author each, with only four authors producing two publications. A study of the citations found that the top citing publication was (Martí-Parreño et al., 2016) with 63 citations. However, it was difficult to select another based on the number of citations as, for example, the second top-cited publication with 27 citations explored the field of educational technology since 1970 and not relevant. Further review found a second publication, Trinidad et al. (2021), with two citations. Other searches outside the Web of Science found another publication Luo (2021), with one citation. Table 2.2 summarises the three bibliometric analyses, and all three used Web of Science for searches.

The analyses of the three bibliometric publications (see Table 2.2) had very similar results for the top three journals. Two had the same two in positions one and two and the third the same two in reverse order. There were differences in leading scholars' selection, despite similar search terms. However, Martí-Parreño et al. sample size were approximately less than 4% of Trinidad et al. or Luo. Review of Arnab S, who is the top for citations in Lou (analysis period: 1995-2020), started publishing in 2016 and has contributed regularly since then. The different search dates and more complete search terms would explain the difference between Trinidad et al. (2021) and the Luo (2021) order of leading scholars.

[5] https://www.webofscience.com/
[6] https://scholar.google.com/

Table 2.2: Summary Bibliometric Analysis.

Description	**Martí-Parreño et al. (2016)**	**Trinidad et al. (2021)**	**Luo (2021)**
Analysis period	2010-2014	1900-2019	1995-2020
Sample size	150	4,706	4,059
Data Collection	Web of Science	Web of Science	Web of Science
Keyword search	'game-based learning' or 'serious games' or 'gamification'	'gamification', 'gamify', or 'gamifying'	'gamification' or 'gamify' or 'gamified' or 'gamifying' or 'serious game' or 'gameful design' or 'game-like' and ('education' or 'learning' or 'teaching').
Top Journals	**Sample of Top Journals**	**By Citations**	**By Citations**
1st	Computers & Education	Computers in Human Behavior	Computers & Education
2nd	Computers in Human Behavior	Computers & Education	Computers in Human Behavior
3rd	Three journals same score	International Journal of Human Computer Studies	Three journals similar scores
Leading scholars	**By Citations**	**By Citations**	**By Citations**
1st	Hwang, Gwo-Jen	Hamari J	Arnab S
2nd	Chu, Yu-Ling	Koivisto J	Fernandez-Manjon B
3rd	Liu, Tsung-Yu	De-Marcos L	Hauge JB

The next stage was to verify recent trends to verify the top authors and journals as Luo (2021) did not include 2021 publications. The new date range for publications to concentrate on the last six years between 2016 and 2021.

2.4.2 Find Top Authors and Publications in Gamification 2016 - 2021

The Web of Science was searched again using the inbuilt search function using a similar keyword search Luo (2021). The first decision was the keywords to include in the search term. It was noted in Table 2.2 the Luo (2021) search used a more comprehensive range of search terms than both Martí-Parreño et al. (2016) and Trinidad et al. (2021), and later search used the additional keyword 'game-based learning'. Khan et al. (2011) search of bibliometric analysis on the research trends of gamification in higher education 2010 -2020, found the top keyword occurrences used

by authors (n>11). These keywords include ‘motivation’, ‘game-based learning’, ’e-learning’, ‘serious games’, and ‘learning’. Search terms one and two completed with the date range were 01/01/2016 to 31/12/2021.

Gamification Publication Trends Search One: *(TS=(gamification) OR TS=(gamify) OR TS=(gamified) OR TS=(gamifying) OR TS=("serious game") OR TS=("gameful design") OR TS=("game like")) AND (TS=(education) OR TS=(learning) OR TS=(teaching)).*

The search produced 5,445 publications and a second search completed included the missing term ‘game-based learning’ used in Martí-Parreño et al. (2016) and found as a keyword used by authors in bibliometric analysis by Khan et al. (Khatibi et al., 2021).

Gamification Publication Trends Search Two: *(TS=(gamification) OR TS=(gamify) OR TS=(gamified) OR TS=(gamifying) OR TS=("serious game") OR TS=("gameful design") OR TS=("game like") OR TS=("game-based learning")) AND (TS=(education) OR TS=(learning) OR TS=(teaching))*. The search produced 7,139 publications. See Figure 2.3 for summary by year by publication and citation and adding search term ‘game-based learning’, added 1,694 publications from search one.

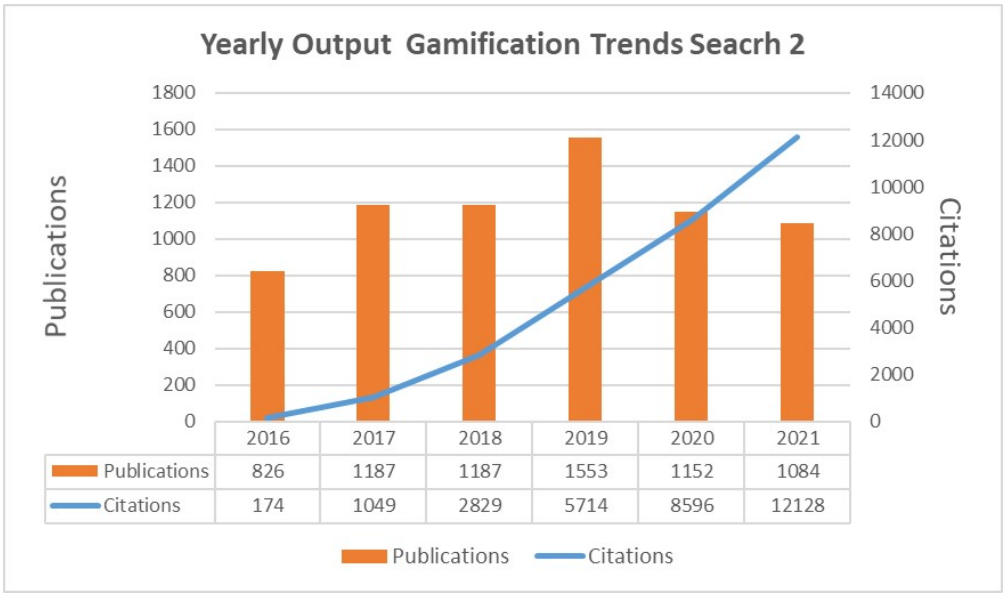


Figure 2.3: Gamification Publication Trends include search term ‘game-based learning’ (Web of Science 2016 - 2021).

The second search term was used for further analysis. Figure 2.3 shows the increase in publications from 826 in 2016 to 1,553 in 2019, then dropping to 1,152 in 2020 and 1,084 in 2121. However, the citations have increased, from 174 in 2016 to 12,128 in 2021. The drop-in publications were possibly Covid-19 related as often a requirement for testing serious games required presence, even for online games tests and this was restricted during the pandemic. However, with some exceptions, SherLOCKED game (Jaffray et al., 2021) was created during Covid-19 to increase student engagement with university cyber courses when the students were moved to online lectures.

The top publications by citations were Computers & Education and second place Computers in Human Behavior (see Table 2.3). These were the same positions as Trinidad et al. and Luo from the bibliometric analyses (see Table 2.2).

Table 2.3: Gamification Trends Top Publications by Citation (Web of Science 2016 - 2021).

		Citing Articles		Times Cited			
Publication	**No**	**Total**	**Without Self-Citations**	**Total**	**Without Self-Citations**	**Average per item**	**H-Index**
Computers & Education	91	1,883	1,843	2,482	2,394	27.27	30
Computers in Human Behavior	64	1,913	1,896	2,330	2,300	36.41	23
Interactive Learning Environments	73	702	681	811	781	11.11	15
Educational Technology & Society	44	505	495	575	562	13.07	15
International Journal of Educational Technology In Higher Education	14	445	441	472	467	33.71	9

The top author by citations gave a different range because of the broader search term and defined six-year date range from 2016 to 2021, see Table 2.4. For example, Arnab S, with 149 total citations, is in the seventh position, whereas in Luo bibliometric analyses, he is the first place. It is noted that Hwang GJ, who is in the top position, used the term 'game-based-learning' in his publications. This term was not used by Luo (2021) but by Martí-Parreño et al. (2016), who also placed Hwang GJ in the top position.

Table 2.4: Gamification Trends Top Author by Citation (Web of Science 2016 - 2021).

		Citing Articles		Times Cited			
Author	**No**	**Total**	**Without Self-Citations**	**Total**	**Without Self-Citations**	**Average per item**	**H-Index**
Hwang GJ	28	386	376	444	425	15.86	11
Ninaus M	30	145	121	194	140	6.47	7
Marti-parreno	21	175	170	188	183	8.95	7
Moeller K	20	129	114	169	134	8.45	7
Kiili K	20	124	108	169	128	8.45	5
Iostani S	23	138	125	164	137	7.13	8
Arnab S	30	140	129	149	135	4.97	5
Fernandez-manjon B	20	78	71	108	89	5.4	6
Lester J	20	99	92	123	107	6.15	6

2.4.3 Find Pedagogical Design Models for Serious Games

The serious games search also tried to find any pedagogical models used to design the games. Search term two was modified to include keywords found in published pedagogical models.

Serious Games Design Search *((TS=(gamification) OR TS=(gamify) OR TS=(gamified) OR TS=(gamifying) OR TS=("serious game") OR TS=("serious games") OR TS=("gameful design") OR TS=("game like") OR TS=("game-based learning")) AND (TS=(pedagogical) OR TS=(pedagogy) OR TS=("Game object model") OR TS=("assessment learning in games") OR TS=(“serious games analysis”)))*

This search resulted in 1,271 publications, starting in 1995 with first publication, and next publication in 2005, see Figure 2.4.

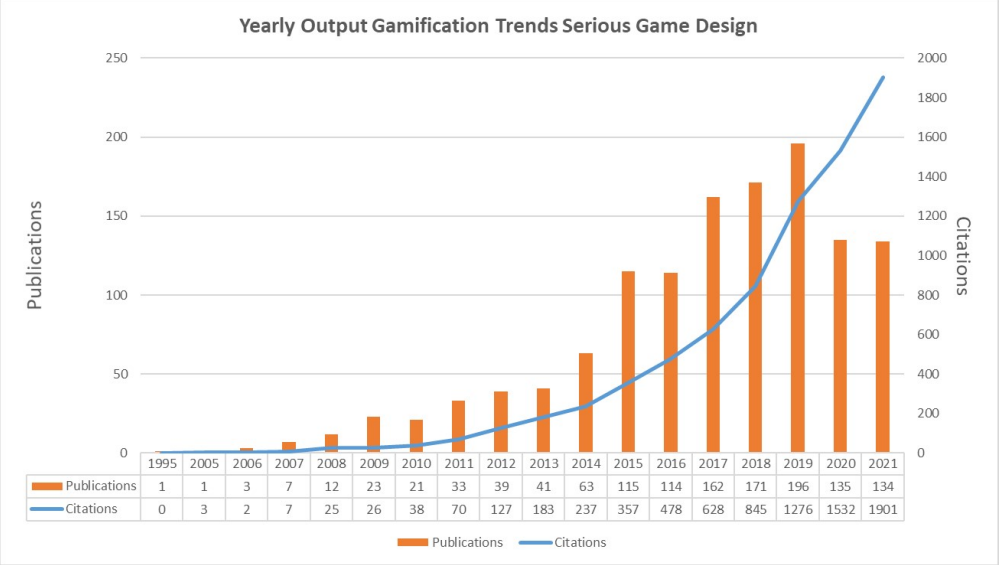


Figure 2.4: Gamification Publication Trends Serious Games Design (Web of Science 1995 - 2021).

The top three authors by H-Index of 7 (see Table 2.5) were Arnab S, Belotti F and Berta R. Search for the top-cited papers overall found following top six publications:

1. Neck and Greene (2011), Entrepreneurship Education: Known Worlds and New Frontiers, cited 476,
2. Arnab et al. (2015), Mapping learning and game mechanics for serious games analysis, cited 273.
3. Liu and Chu (2010), Using ubiquitous games in an English listening and speaking course: Impact on learning outcomes and motivation, cited 267.
4. Moreno-Ger et al. (2008), Educational game design for online education, cited 231.
5. Hainey et al. (2016), A systematic literature review of games-based learning empirical evidence in primary education, cited 148.

6. Carvalho et al. (2015), An activity theory-based model for serious games analysis and conceptual design, cited 127.

Following a review of the six top-cited papers. **1.** Neck et al. publication is about entrepreneurship courses and was rejected. **2.** Arnab et al. was selected as a base for research into pedagogical models for serious games, see Chapter 6. **3.** Liu et al. study investigates how ubiquitous games affect learning outcomes and was rejected. **4.** Moreno et al. is about requirements for the design of educational games in online context only and rejected. **5.** Hainey et al. is a systematic literature review of game-based learning and rejected. **6.** Carvalho et al. activity theory will be used to design a new pedagogical model, see Chapter 7.

Table 2.5: Pedagogical Models for Serious Games Design Citation Report (Web of Science 1995 -2021).

		Citing Articles		Times Cited			
Author	**No**	**Total**	**Without Self-Citations**	**Total**	**Without Self-Citations**	**Average per item**	**H-Index**
Arnab S	18	402	393	447	434	24.83	7
Bellotti F	12	449	444	520	513	43.33	7
Berta R	12	461	457	529	524	44.08	7
Ott M	10	115	112	119	114	11.9	5
Albert D	14	104	97	109	102	7.79	4
Lim T	10	354	347	386	375	38.6	4
Hauge JB	12	150	147	152	148	12.67	3
Artal-Sevil JS	10	13	7	31	8	3.1	3

2.4.4 Conclusion of Searches

The search for top authors and journals from the bibliometric analysis in subsection 2.4.1 identified Computers & Education[7] and Computers in Human Behaviour[8] (both published by Elsevier) as the top two journals and top three authors Arnab S, Fernandez-Manjon and Hauge JB. Further searches of Web of Science in subsection 2.4.2 cover recent years 2016-2021 with broader search term found a more comprehensive range of possible authors with similar H-Index, see Table 2.4. The bibliometric analysis and second direct search comparison confirmed the two top publications. The last more refined search for pedagogical models to design and assess serious cyber games in subsection 2.4.3 identified three top authors with the same H-index of 7. Arnab S with 18 publications, Bellotti F with 12 publications and Berta R with 12 publications (Table 2.5). The publication from Arnab was the most relevant to the research objectives (Arnab et al., 2015) and the second-highest cited paper.

The publishers, journals, and authors found following these searches can be used to find relevant papers on gamification and serious games to be reviewed. However, the search term can make a

[7] https://www.journals.elsevier.com/computers-and-education
[8] https://www.journals.elsevier.com/computers-in-human-behavior

considerable difference in search results. The first search one found 5,445 publications but, when adding 'game-based learning', found additional 1,694 publications in search two.

2.4.5 Searching for Serious Cyber Games and Testing

The search in subsection 2.4.1 and subsection 2.4.2 found some of the top authors and publications in gamification using keyword searches. However, most serious games are published by authors who may only publish one game and may not be in the top authors or publications list by citation. An alternative search strategy was using top publishers found from search 2 (subsection 2.4.2). Example of the top four publishers IEEE[9], Springer[10] (Springer Nature), Int Assoc Technology Education & Development (IATED)[11] and Elsevier[12].

It should be noted there are other sources with lists of possible serious games published by leading experts. For example, Adam Shostack, a leading expert on threat modelling and game designer, publishes a list of security educational games[13].

If the serious game found in the literature review was available to play online or was available to purchase as a physical game, then the game was purchased for evaluation, with some exceptions. Only two of the games were available to play online. LINDDUN GO, which was for sale as a card game and available free online[14], and Elevation of Privilege (EoP)[15], which is also available to purchase and online. It was possible to evaluate other games through published research and scholarly journals. Table 2.6 lists all the serious games available to buy, download or play online. The serious games selected to be played or reviewed to understand the gameplay and mechanics are detailed in Section 2.5.

Table 2.6: Serious Cyber Games Available To Purchase, Download or Play Online.

Game	Type	Available	Comments (Cost exclude postage)
Elevation of Privilege see subsection 2.5.1	Card Set	Purchase Download Online	Buy online for £16.99, download or play online
OWASP Cornucopia, see subsection 2.5.2	Card Set	Download	Download & self-print cards (Sometimes available online to purchase)

Continued on next page

[9] https://ieeexplore.ieee.org/Xplore/home.jsp
[10] https://link.springer.com/
[11] https://iated.org/publications
[12] https://ieeexplore.ieee.org/Xplore/home.jsp
[13] https://shostack.org/games.html
[14] https://www.linddun.org/go
[15] https://eopgame.azurewebsites.net

Table 2.6 – continued from previous page

Game	Type	Available	Comments (Cost exclude postage)
Hacker, see subsection 2.5.4	Board Game	Purchase	Buy online $36.96
Decisions & Disruptions, see subsection 2.5.8	Lego® Game	Download	Download & self-print cards and buy Lego® online
Control-Alt-Hack, see subsection 2.5.9	Card Set	Purchase	Buy online $30.00
[dox3d!] see subsection 2.5.10	Tile & Cards	Download	Download & self-print
Cryptomancer RPG, see subsection 2.5.11	Instructions	Purchase	Buy online instructions run to 440 pages
Cyber Threat Defender, see subsection 2.5.12	Card Sets	Purchase	Buy online $24.00 for two starter decks
Exploit!, see subsection 2.5.13	Purchase	Card Set	Buy online $23.99
The Security Cards, see subsection 2.5.18	Card Set	Purchase	Buy online $19.00
Crypto Go, see subsection 2.5.19	Card Set	Download	Download & self-print cards
LINDDUN GO, see subsection 2.5.20	Card Set	Purchase Download Online	Buy online £15.99 and play free online

2.5 Serious Games for Cyber Security

This section gives a brief description of the gameplay for each game identified for initial review. We are looking for games that have been designed using the research aims and objectives in Section 1.3.

2.5.1 Elevation of Privilege (EoP)

Description: The EoP (Microsoft, 2018; Shostack, 2014) is a card game proposed by Microsoft to conduct threat modelling as part of the design phase of software projects. The EoP game is

available to purchase[16] for approximately £16.99 (excluding postage correct as of 09/01/2022) and also download to self-print[17].

Number of Players: 1-5

Brief Description of Gameplay

Playing Cards – Single card deck with 74 cards in six suits, based on Microsoft STRIDE threat categories[18], see Figure 2.5 for sample of cards.

Figure 2.5: Elevation of Privilege Example Cards (Shostack, 2014)

- Spoofing - 2 to 10, Jack, Queen, King Ace (13 cards)
- Tampering - 3 to 10, Jack, Queen, King Ace (12 cards)
- Repudiation - 2 to 10, Jack, Queen, King Ace (13 cards)
- Information Disclosure - 2 to 10, Jack, Queen, King Ace (13 cards)
- Denial of services - 2 to 10, Jack, Queen, King Ace (13 cards)
- Elevation of Privilege (EoP) - 5 to 10, Jack, Queen, King Ace (10 cards)

Gameplay - Draw a diagram of the system that you want to use as a threat model

- Deal all the cards to the players
- Play starts with whoever has the 3 of Tampering Card
- Play is clockwise (players can help each other by facing cards up in suit order)
- Have all players played in this hand?

  No – continue play

[16] https://agilestationery.com/products/elevation-of-privilege-game
[17] https://www.microsoft.com/en-gb/download/details.aspx?id=20303
[18] https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

Yes – After each player has played a card, the trick is won by the player who has played the highest card in either the suit led (first card) or in the 'trump' suit, Elevation of Privilege. The highest card is the highest value card played in the suit led unless one or more trump cards[19] were played. If a trump card has been played, the highest value trump card is the winning card.

- Play then proceeds with the player who won the previous trick. That player leads the next trick by selecting a card from his hand and playing it as above.
- The player looks for a card to play (players can sort cards into suits and play face up)

  Do you have a suit of the first card that was played? Yes, you must play one of these cards. Could play a low card where you know the threat to win a point. Could play the Ace to try and take the trick, you might not know the threat, but strategy to win the trick point to take the lead on the next hand. It only works if the Ace is in a suit that led the hand and trump is not played as if a trump card is played, then the highest trump card would win the trick, and you wasted playing your Ace.

  No, do you have an EoP card? *Yes*, you may play this card. No, play a card in another suit

Awarding Points

- The player reads the card, and for 1 point to explain the threat on your card against the diagram in item 1, the threat is recorded in the score sheet. If a player cannot link the threat, the play continues
- The Elevation of Privilege (EoP) card or suit lead (the Ace) takes the trick for 1 point (additional point if they can explain the threat) – cannot be played if you have a suit of the card previously played.

EoP Game update. The EoP game has been updated to add a privacy suit[20], see Figure 2.6.

Figure 2.6: Elevation of Privilege (EoP) Game Threat Modelling Cards - with Privacy.

[19] https://en.wikipedia.org/wiki/Trump_(card_games)
[20] https://agilestationery.com/products/elevation-of-privilege-with-privacy-suit?

2.5.2 OWASP Cornucopia

Description: OWASP Cornucopia (OWASP, 2021) is a card game used to help derive application security requirements during the software development life cycle. The game is available from OWASP website to download for self-printing[21].

Brief Description of Gameplay

This game was based on the Microsoft EoP card game (Microsoft, 2018; Shostack, 2014). Instead of the six Spoofing, Tampering, Repudiation, Information Disclosure & Elevation of Privilege (STRIDE) suits, the game is based on:

- OWASP secure coding practices quick reference guide (SCP)
- OWASP Application Security Verification Standard (ASVS)
- OWASP AppSensor - Application Layer Intrusion Detection
- The Common Attack Pattern Enumeration and Classification (CAPEC™)
- OWASP SAFECode

Figure 2.7 an example of 7 of Authentication card, Jack of Cryptography and Ace of Data Validation & Encoding. All cards have references to the appropriate standards in SCP, ASVS, AppSensor, CAPEC, and SAFECode. Each suit has an Ace card with the same rule as EoP and allows players to invent a new attack based on the category of the card.

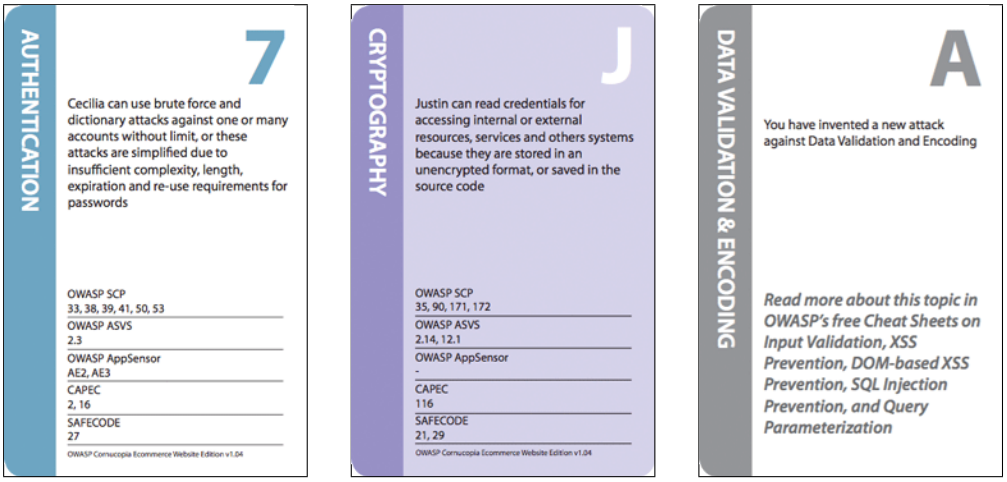


Figure 2.7: Example Cornucopia Game Cards (OWASP, 2021).

The card deck is based on 78 cards in six suits (13 cards per suit):

1. Data validation and encoding
2. Authentication
3. Session management
4. Authorisation

[21] https://owasp.org/www-project-cornucopia/#div-cards

5. Cryptography
6. Cornucopia ('Cornucopia' suit was created for everything else)

Gameplay

- Diagram used is a Data Flow Diagram (DFD) created for the game
- Play is clockwise round the table
- Cards are in suits with high cards being Jack, Queen, King and Aces
- All cards are dealt to the players, but they play holding the cards
- Players like EoP must follow the suit of the card played
- Get a point for identifying a vulnerability
- If you do not have a card of a suit in play, you can play any other card but will not win the hand
- End of the round, when each player has played a card, the highest suit of the first card played wins the round, and a point
- The outcome will be a list of security requirements or threats that need to be reviewed later
- The outcome is converted into user requirements
- The game does not have trump cards like EoP
- Like EoP at the end, points are added up to find the winner

2.5.3 Protection Poker

Description: Protection Poker (Williams et al., 2010) game is based on hypothetical health system database tables called iTrust.

Brief Description of Gameplay

- Patients can see and manage their medical records
- Medical personnel can manage the medical records of their patients
- Alerts of patients with warning signs of chronic illness or missing immunisations
- Perform bio surveillance such as epidemic detection

Calculation of risk is based on the formula: Risk = ((probability of loss) x (impact of loss))

Gameplay goes through four steps to create a prioritised list with ranking risks linked to iTrust requirements.

Step 1 **Value and rank your software assets** - calibrate *'Asset Value Points'* given list of tables rank the table in database least valuable to the attacker and mark this one and the use poker cards to agree on the ranking number of most valuable table in a database and mark these up to 100, see extract Table 2.7

Step 2 **Calibrate the ease of attack** for new requirements calibrate *'Ease Points'* given list of requirements, for example, view a log, use the same technique as in step 1 to rate all the

requirements from the hardest (score 1) to the most effortless requirement to attack (score up to 100)

Step 3 Compute the security risk

Identify which assets are used in the new features, see column 'Used in Feature', Table 2.7

Add up the total value points mapped to each feature and record that sum, see column 'Total Value Points', Table 2.8

Add up the ease points mapped to each feature and record that sum, see column 'Ease Points', Table 2.8

Table 2.7: Protection Poker Game Summary Points Table.

Asset Value Point	Customer Data	Used in Feature
2	Customer login ID	
5	Customer password	
8	Email	2,3
3	Customer name (first)	2,3
8	Customer name (last)	2,3
20	Credit card ID	
40	Credit card PIN	
20	Driver's license or passport	
1	Customer #	1,2,3
2	Known allergies	1,2
8	Customer group	3
8	Customer group #	3

Table 2.8: Protection Poker Game Summary Feature 2 Highest Risk.

Feature	Total Value Points	Ease Points	Security Risks
1	3	1	3
2	22	5	22 x 5 = 110
3	36	3	108

Rank security risk – Security Risk = (('Ease Points') x ('Value Points')), see extract Table 2.8, where feature 2 has the highest risk. Asset Value Total Points = 22 x Ease Points = 5 = Total Security Risks 110

Step 4 Add mitigation to the iteration In this step, your team decides what goes into the next iteration to mitigate the risk

2.5.4 Hacker

Description: Hacker (ThinkFun, 2021) is a coding board game used to defend against attacks from cybercriminals by joining a white hat hacker team and playing the role of a coder, hacker,

and security engineer. The game has 40 challenges from beginner to expert. The Hacker game is available to purchase[22] for approximately $36.96 (excluding postage correct as of 09/01/2022).

Number of players: 1 or more

Brief Description of Gameplay

Setup board with one of the 40 challenges. See Figure 2.8 for an example of a challenge with missing steps 1, 2 and 4.

Figure 2.8: Hacker Game Challenges Booklet (ThinkFun, 2021).

***Phase 1* – Code It:** Program the agents to pick up data files and reach exit points. Each program has a control panel between four and ten steps. Figure 2.10 shows the moves from the control panel in Figure 2.9. The instruction is to either move the blue, red agent or turn one of the four coloured platforms 90 degrees clockwise or anti-clockwise following tile on the program step.

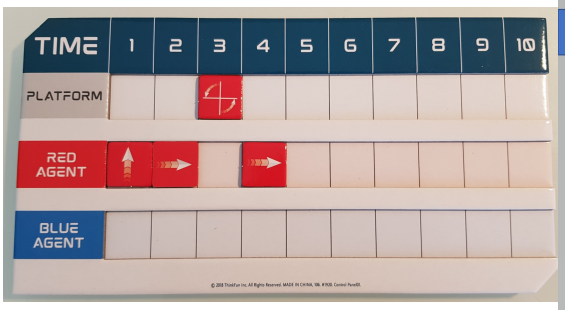


Figure 2.9: Hacker Game Control Panel (ThinkFun, 2021).

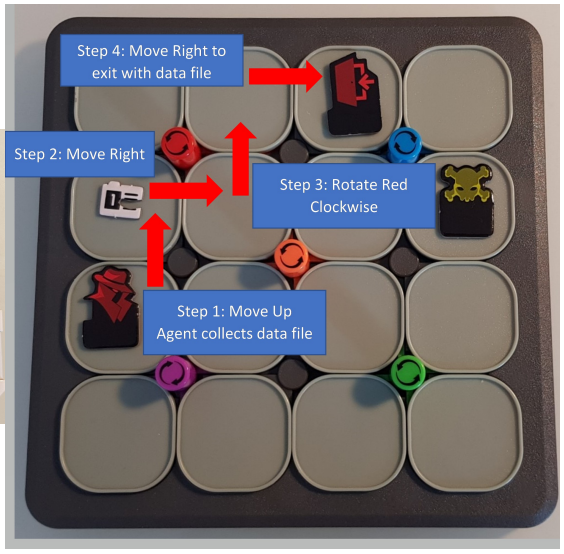


Figure 2.10: Hacker Game Platform (ThinkFun, 2021).

***Phase 2* – Hack It:** Analyse the program created in phase 1 and find security vulnerabilities. Analyse the program and find a way to move the agent tiles to reach the virus token, and you win by infecting the control system.

[22] https://www.amazon.com/gp/product/B07FXYJ5BC/

***Phase 3* – Fix It:** Change the program you created in phase 1 to prevent vulnerability found in phase 2. Prevent the attack by placing an alarm token preventing the agent from reaching the virus. See *Hack IT* and *Fix IT* examples in Figure 2.11 of code created in Figure 2.9 & Figure 2.10.

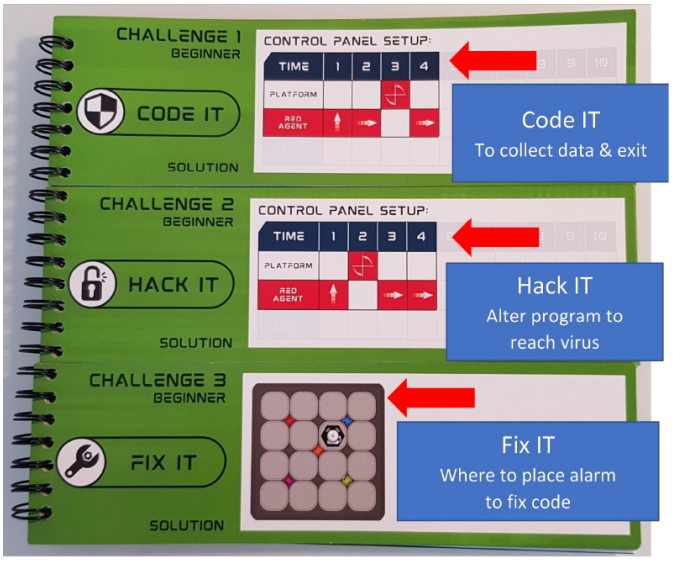


Figure 2.11: Hacker Game Solutions Booklet (ThinkFun, 2021).

2.5.5 CyberCIEGE

Description: CyberCIEGE (Irvine et al., 2005; Thompson and Irvine, 2011) is an educational video game. The U.S. Navy sponsored its development. It is used as a training tool by agencies of the U.S. government, universities, and community colleges to offer an environment for the simulation of office scenarios for the cyber education of employees. CyberCIEGE scenarios cover network management, network filters, Virtual Private Networks (VPNs), e-mail encryption, access control mechanisms, biometrics, and Public Key Infrastructure (PKI). Players must balance the budget to productivity and security by keeping the virtual world's personal and data safe whilst protecting assets from cyber attacks.

Number of Players: 1

Brief Description of Gameplay CyberCIEGE is an interactive environment, and Players of this video game purchase and configure workstations, servers, operating systems, applications, and network devices. See Figure 2.12 for an example of the configuration of VPN. The players must make trade-offs between budget, productivity, and security. The players can advance through stages with escalating attacks. See Figure 2.13 for an example of a Malware attack.

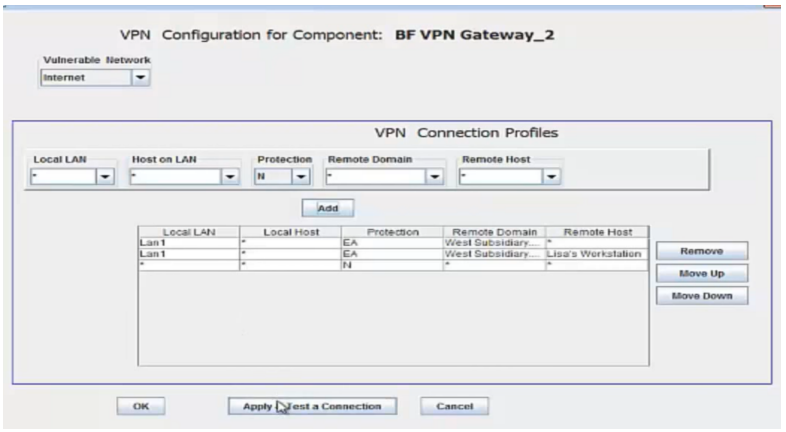


Figure 2.12: CyberCIEGE Game Screenshot VPN Configuration (Irvine et al., 2005; Thompson and Irvine, 2011).

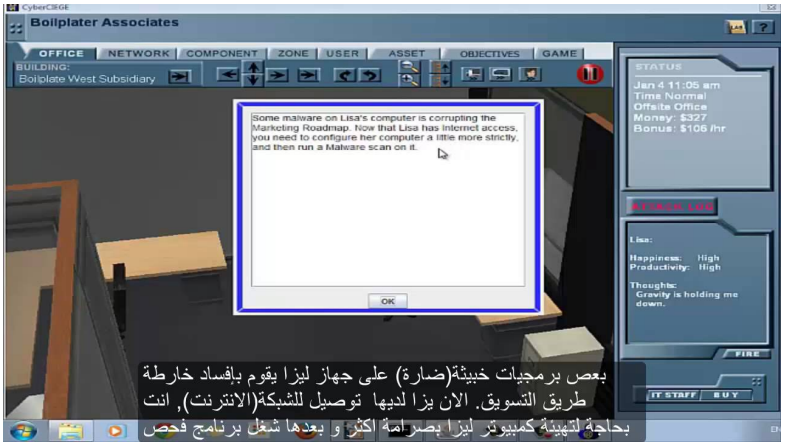


Figure 2.13: CyberCIEGE Game Screenshot Example Malware Attack (Irvine et al., 2005; Thompson and Irvine, 2011).

2.5.6 PERSUADED

Description: PERSUADED (Aladawy et al., 2018) is a computer game that allows players to learn the effectiveness of defence controls against most common social engineering attacks.

Number of Players: 1

Brief Description of Gameplay

Four types of cards - Attack, Defend, Future and Skip a Turn.

1. Attack cards include attack scenarios in textual form.
2. Defence cards describe a pattern of behaviour that protects the player against an exploitation attempt. A defence card exists for each attack card.
3. See the Future cards allow the player to 'take a peek' at the three upper cards in the card deck.
4. Skip turn cards allow the player to take the upper card of the deck and put it below the deck.

Figure 2.14: PERSUADED Game Four Types of Cards (Aladawy et al., 2018).

Game Mechanics - is based on a single-player game like patience and solitaire, where the player can decide to play a card in their hand or draw another card from the deck.

1. Play an action card or draw a card from the deck.
2. If you draw any card that is NOT an Attack, the turn is over. Put the card to your hand cards.
3. If you draw an Attack card, you must play a Defence card. The correct defence gains you 10 points, and the wrong defence loses 5 points. The Defence card is only discarded if you had a correct match. Otherwise, it is put back in the deck.
4. If you draw an Attack card and do not have any Defence card in your hand, you lose one heart (life). If you lost all three of your hearts, the game is over.
5. The game is won if the deck is empty and is lost if the player loses all three lives before finishing the deck.

2.5.7 Cyber Security Requirements Awareness Game

Description: Cyber Security Requirements Awareness Game (Yasin et al., 2019) is a tabletop card game developed to educate cyber security risks in hospital-related scenarios.

Number of Players: Teams of 3 to 4

Brief Description of Gameplay
The Game Board is based on the security context mimicking a hypothetical organisation with a floor plan and the potential assets to be protected (see Figure 2.15). The *Security Context* of the game is based on the team players belong to the undercover team of a Health IT systems security agency. The Agency has received Intelligence that one particular hospital is the target of a ransomware attack. *Teams of players* are three to four. The first player acts as the role of Network attacker, the second of Social Engineer Attacker, and the third role of Physical Attacker. One to one mapping was performed for the game assets or elements, see Figure 2.16. Some of the concepts are mapped directly, for example the process of solving a puzzle card to get access to the room.

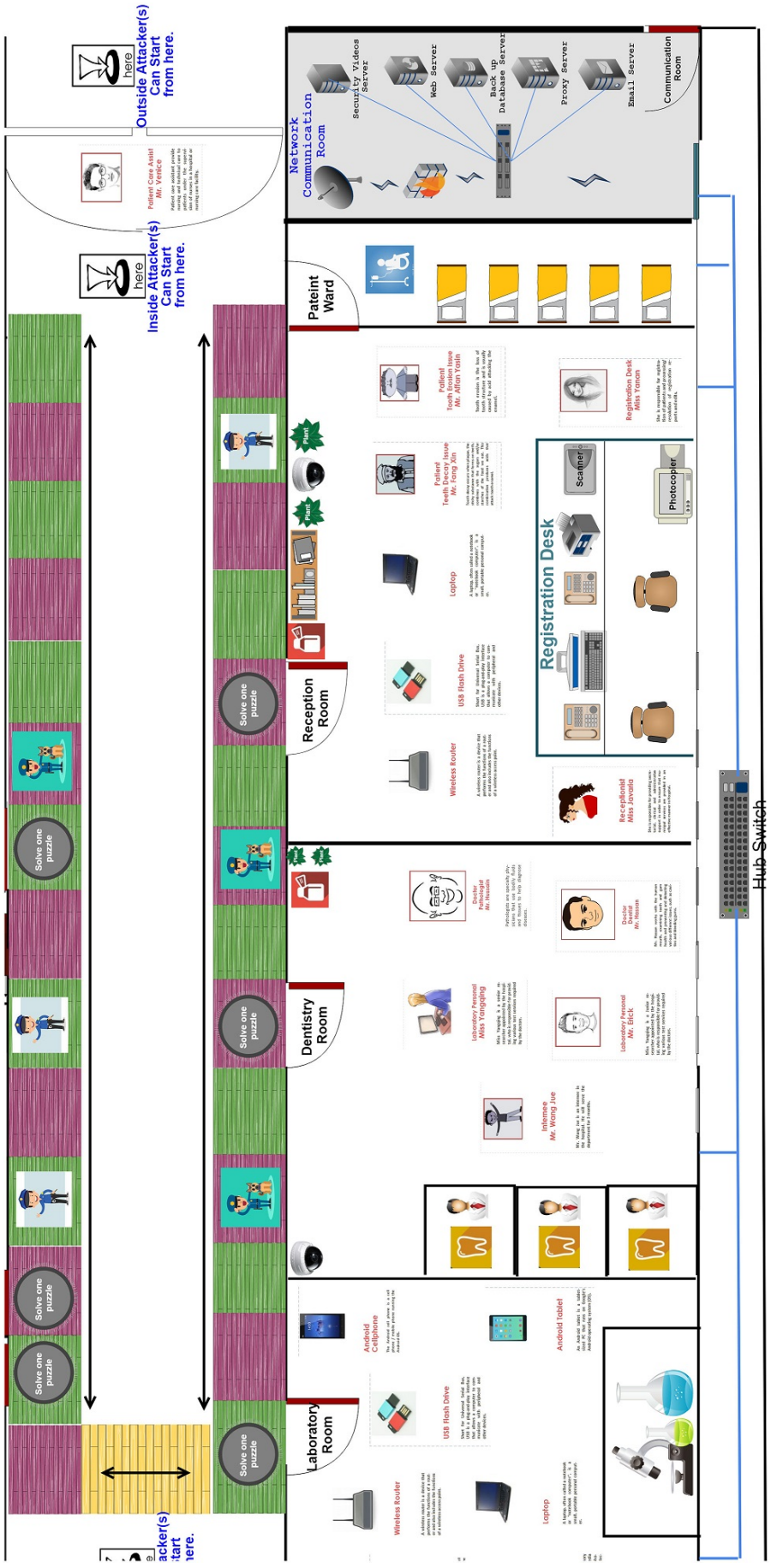


Figure 2.15: Cyber Security Requirements Awareness Game - Game Board Map of the (Partial): Hospital information systems (Yasin et al., 2019).

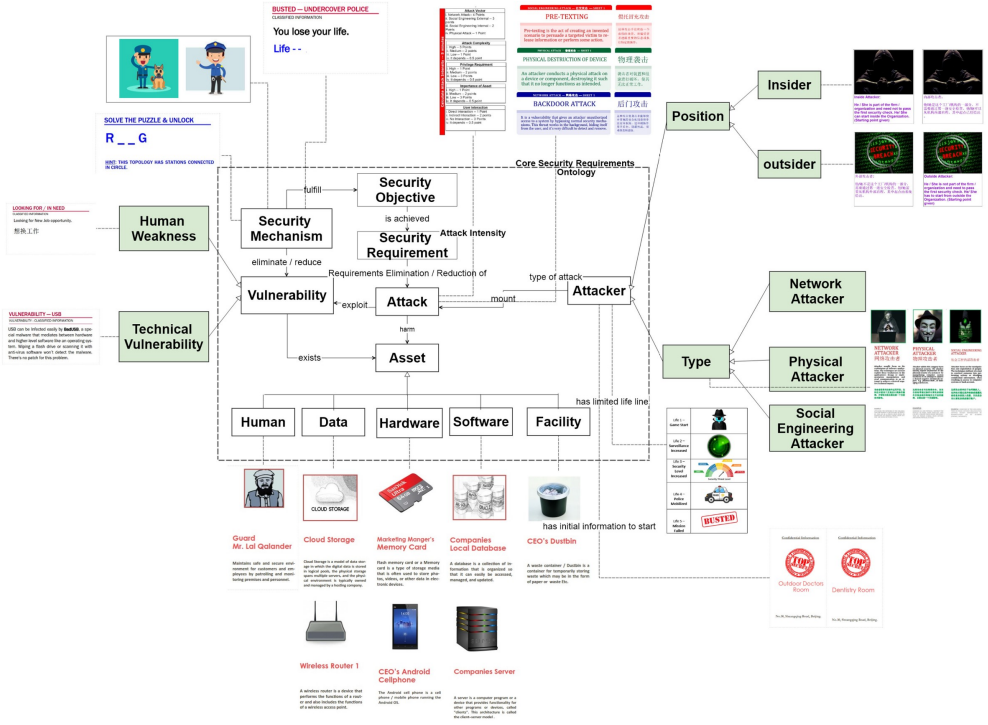


Figure 2.16: CSRAG Game Structure and the Corresponding Game Cards (Yasin et al., 2019).

The Gameplay

Step 1 Select Room from Map - Player selects which room they are going to attack

Step 2 Select Insider or Outsider Attacker - Player decides if inside or outside attacker, and if outside must compromise person by the entrance

Step 3 Roll the Dice - Player rolls dice to move on the map

Step 4 The puzzle - Solve the puzzle to gain access to a room

Step 5 Selection of spy - A player random selection which asset is the spy and, if correct, get direction to an infected device and, if not correct, loses a life

Step 6 See vulnerability and Description of the Asset - Player proposes a viable attack

Step 7 Propose Hypothetical Scenarios - after devising the attack, the player of the team must write a hypothetical scenario for the attack

Step 8 Discussion / Review between teams - discussion session between the teams will start to improve further scenarios and give points to them

2.5.8 Decisions & Disruptions

Description: Decisions and Disruptions (Frey et al., 2017) game is based on using Lego® to describe a small utility company with two locations, first field site where it runs the plant and second location an office. The game tasks a group of players with defending the security of the utility company within a given budget. See Figure 2.17 for the Decisions & Disruptions Board.

Two recent versions of Decisions & Disruption were updated to include privacy threats from General Data Protection Regulation (GDPR) (Shreeve et al., 2020).

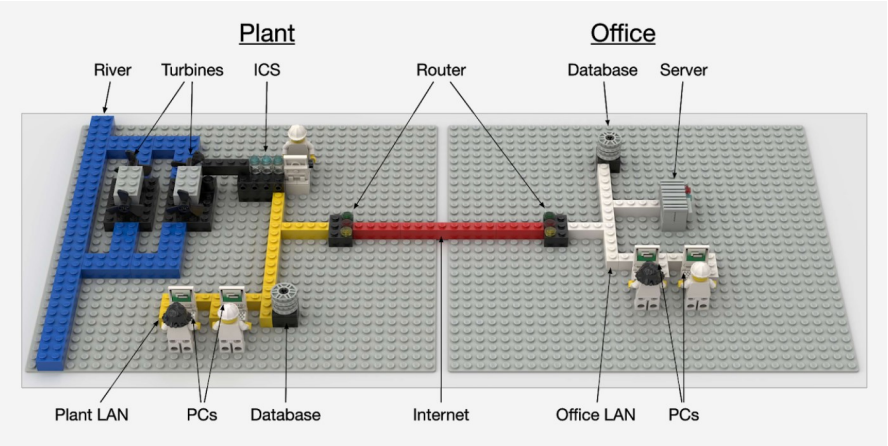


Figure 2.17: Decisions & Disruptions Lego® Game Board (Frey et al., 2017).

The game cards and instruction booklet is available to download[23] for self-printing, with a list of Lego® pieces you need to create the game board[24].

Number of Players: 2-6 players

Brief Description of Gameplay

Decisions & Disruptions (D-D)[25] is a turn-based game, where each turn represents approximately two months in the D-D world. A complete D-D session lasts four turns. Each turn follows the same structure:

1. **Setup – turn**
   (a) Setup game board
   (b) The Game Master describes the game situation to the players: the state of their infrastructure, known threats and ongoing attacks
   (c) Advise they have a budget of 100,000 credits (per turn)
   (d) Place first set of defence game cards face up (hold back five cards: two defence cards and three encryption cards)
   (e) Describe the defence cards

[23] https://github.com/benshreeve/decisions-disruptions-kit
[24] https://www.bricklink.com/v3/studio/design.page?idModel=55446
[25] Game rules available at: https://www.decisions-disruptions.org/

2. **Defence**
   (a) The players agree to decide by to consensus where to spend their 100,000 budgets
   (b) Remove cards from the table and deploy the defences on the game board in Lego

3. **Consequences**
   (a) Game Master explains the consequences of defence decisions (see Figure 2.18) about the effects of their investments: whether their defences deflect any attacks, and the effects of undefended attacks

4. **Attack**
   (a) Describe to the players what happens during the two months following their investments, the attack and its consequence

5. **Game ends?**
   (a) If turn four, the game ends. If not, go to next turn, step 6 or end game step 7

6. **Next turn**
   (a) Adds 100,000 to budget plus remaining from the previous turn
   (b) Go to step 2

7. **End game**
   (a) At the end of the game, i.e. after turn 4, the Game Master reveals to the players the full range of attackers they were facing, which attacks they deflected successfully and which ones defeated their defences. The end of the game is the stage in which everyone reflects on their decisions and defence strategies

Figure 2.18: Decisions & Disruptions Game Defence Cards (Frey et al., 2017).

Points

- Each successful defence scores 1 point
- State attacks do not count for points

2.5.9 Control-Alt-Hack

Description: Control-Alt-Hack (Denning et al., 2013) is a tabletop card game with: rule book; 3 dice; 156 game cards (16 Hacker, 56 Mission, 72 Entropy, 12 Attendance); 58 Hacker tokens; 42 Money tokens. The game is available from several sources online[26] and currently only available in stock from one source[27] for $30.00, excluding postage correct as of 10/01/2022.

Number of Players: 3-6

Players Age: 14+

Game Time: 1 Hour

Brief Description of Gameplay
Players act as White Hat Hackers working for fun and money. Get enough hacker credits, and you can become the CEO. Mission cards can have two tasks with a score. If negative, then it is a challenging task. For example, you are Hacker Franzi, her skills level on social engineering is 8, but the mission card has plus 3.

Entropy cards add randomness to the game and can be purchased, 'Bag of Tricks Card'. Example Acting Class adds +2 to your social engineering score but will cost you $3,000. 'Light Strike Card' is another Entropy card that you can use against opponents to reduce their skill levels.

Start everyone gets dealt three hacker cards, and they select which one to play. Everyone gets 3 Entropy Cards, 1 Attending Card, 1 Not Attending Card, and 6 Hacker Credits. See Figure 2.19 for an example of each type of card.

Figure 2.19: Control-Alt-Hack Game Cards (Denning et al., 2013) .

[26] http://www.controlalthack.com/buy.php
[27] https://hackerwarehouse.com/product/control-alt-hack/

Phase 1 - Distribute money (some Hackers get more money), and each player draws one Entropy Card.

Phase 2 - Everyone draws their Mission Cards. Next, each play decides if they are going to attend the staff video conference. Attending, draw additional Entropy Card, make a trade or bargain with players to change missions. Not Attending, play the card face down, and you get one free roll of dice during your mission.

Phase 3 - Staff video conference, everyone flips over the attendance card at the same time to see who is attending the staff video conference, leaving the mission card face down. If attending the conference, they flip over their Mission Card and draws 1 Entropy Card. Players attending the video conference can decide to swap missions with other players.

Phase 4 - The Missions, Person with highest Hacker Credit goes first, but as all the same, then it is decided with a roll of 3 dice, and the lowest score wins. However, before the first person plays another player, Lightening Card Example Social Engineering vs roll of the Dice. The Hacker Card Deborah has a Social Engineering Score of 11, so she needs a dice roll of 11 or less for success. Success Lightening Card continues with the mission, but Failure-1 Hacker Credit and then continue with the mission. The player now tries for the first task. For example, Software Wizardry and Deborah have skill level 10, so she needs a dice roll of 10 or less to complete the task. If someone failed a mission got a dice roll higher than skill, they have a second free roll if they decided not to attend the staff video conference meeting. Players could also play one of their Entropy Cards by paying for it, for example, to buy another roll of the dice.

Phase 5 - After all Hackers have attempted their missions

- If only one hacker succeeded, that hacker gets an extra Hacker Credit point
- If only one hacker failed, that hacker loses an extra Hacker Credit point
- If no hacker failed a Mission this round, the entire company reaps the reward: each hacker gets an additional Hacker Credit points

Phase 6 - Discard Entropy Cards. All players must now use or discard cards to get their hand down to 5 (or fewer) Entropy cards

Phase 7 - Check Hacker Credit

- The round is over. Check to see if the hacker with the highest Hacker Credit score has five more points than the next closest rival. If so, that player wins. Game over!
- Otherwise, check to see if the total Hacker Credit score of the company is high enough or low enough that the CEO's position becomes open (see how to become CEO)
- Fired - If your Hacker Credit score is zero at the end of a round, you receive a personal visit from the CEO and you are fired. Draw a Hacker card. Draw three Entropy cards, start with six Hacker Credit points, and see if your new character does better than your last one

Become CEO or CEO Profitable Retirement, the Table 2.9 shows Hacker Credits required:

Table 2.9: Control-Alt-Hack Game - Hacker Credits.

No Players	Fired by CEO	CEO Retirement
3	<12	≤30
4	<16	≤40
5	<20	≤50
6	<24	≤60

2.5.10 [Dox3d!]

Description: [Dox3d!] (Gondree et al., 2013) is a game that is designed to introduce students to network security. The game is currently not available to purchase but can be downloaded[28] for self-printing under a creative commons 3.0 license[29].

Number of Players: 1-4 Players

Brief Description of Gameplay
The game is freely available as open-source, and you can purchase copies for $28.38. Bad guys have stolen your data. As a group, you must hack the network and get your data back. Then escape the network and meet at the internet gateway, then play a Zero-day Card to escape together, and if you do not all escape as a team, you are [Dox3d!].

Board set-up shuffle the [node] tiles, and each square [node] tile represents infrastructure or network service, examples: Web Server, Router, VLAN Switch and other network components, see Figure 2.20 for game board layout example.

Board setup. The nodes start in a white state but, if compromised, are turned over to an orange state (see Figure 2.21 example). The token is placed on [infocon] threat meter with a threat token at the lowest level. The tile colour tracks the status of the network as perceived by network administrators. Next, place the [digital asset drives] card this tracks progress in retrieving your digital assets. Next, place the four tokens that represent the data stolen and two packs of cards, the orange [patch] deck and blue [loot] deck (represent knowledge about exploits), shuffled and room by each deck for a discard pile.

Gameplay. Each player chooses a hacker card that will be their character for the game's duration. Each hacker can infiltrate the network from a different point. For example, the [war driver] can access a wireless router, so card tile is flipped to orange compromised. The hacker's icon is placed on the tile. The game continues by drawing cards, and hackers can only move across the board by compromising nodes adjacent to the tile they are on unless the hacker has a special power to jump two nodes. There order play [action], [loot], [patch], and [check] with players acting in collaboration to recover the stolen data.

[28] https://github.com/TableTopSecurity/d0x3d-the-game
[29] https://creativecommons.org/licenses/by-nc-sa/3.0/deed.en_US

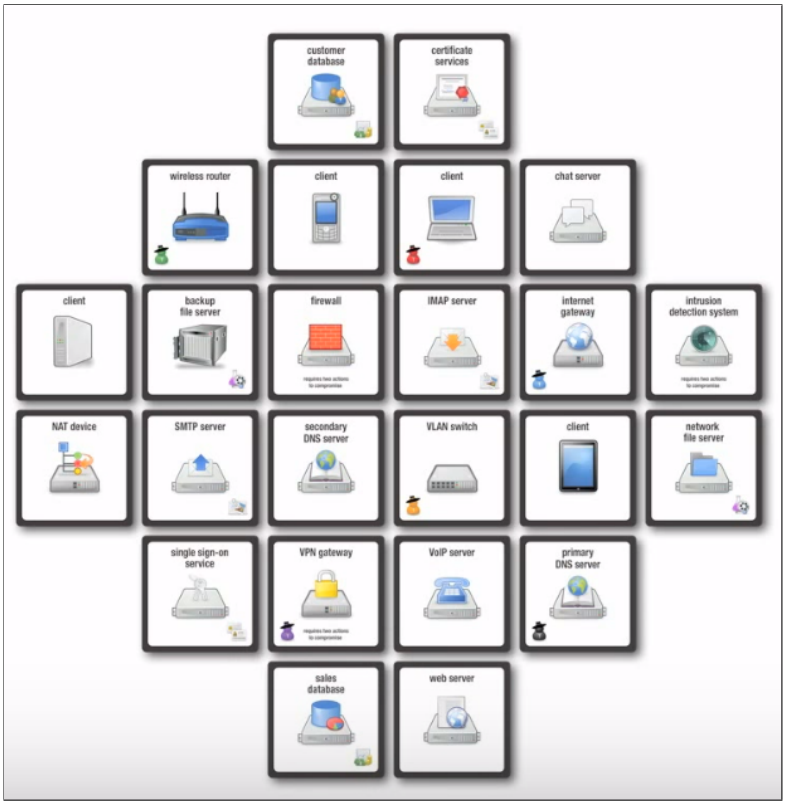


Figure 2.20: [DOx3d!] Game Board (Gondree et al., 2013).

Figure 2.21: [DOx3d!] Game being played at the 2013 US National Science Foundation's Scholarship for Service Symposium (Gondree et al., 2013).

2.5.11 Cryptomancer RPG

Description: Cryptomancer (Cryptomancer RPG, 2018) is a full Role Play Game (RPG) using six-sided and ten-sided dice.

Brief Description of Gameplay

The instructions for the game are in the form of a 430-page PDF, which can be purchased[30] for approximately $19.99 (correct as of 09/01/2022), which also includes Code and Dagger PDFs of 48 and 75 pages. The gameplay requires a skilled Game Master who has played RPG games before. Further information available form website `http://cryptorpg.com/`, see Figure 2.22.

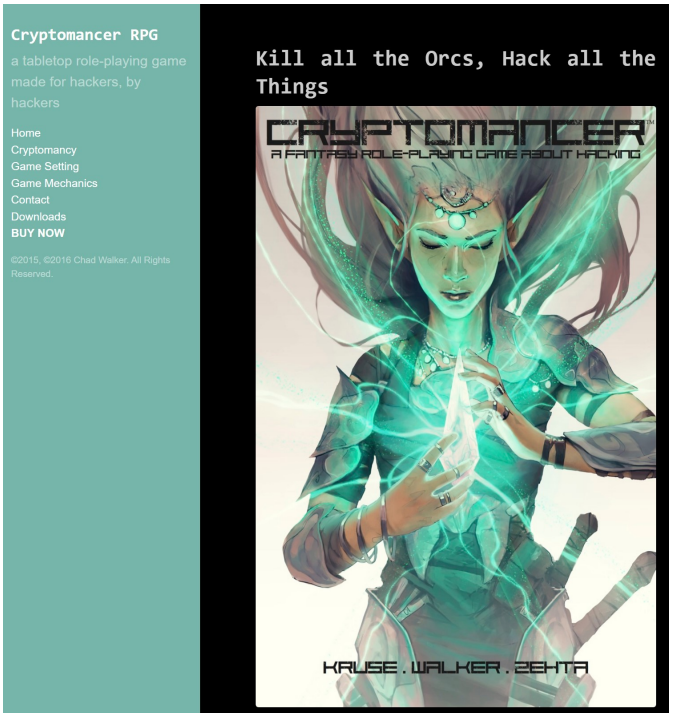


Figure 2.22: Cryptomancer Website (Cryptomancer RPG, 2018).

2.5.12 Cyber Threat Defender

Description: Cyber Threat Defender (Thomas et al., 2019; CIAS, 2021) is a card game based on Assets, Defences and Attack Cards. The game is available to purchase[31] for approximately $24.00 for two starter decks, which includes 54 cards per deck (excluding postage correct as of 09/01/2022).

Brief Description of Gameplay

Cyber Threat Defender is a simple game to understand. The gameplay starts with each player (facing each other) placing down two Asset Cards, Desktop Computer Card and ISP Connection Card. See Figure 2.23 shows the single-player card layout.

[30] `https://www.drivethrurpg.com/product/186678/Cryptomancer`
[31] `https://secure.touchnet.net/C21612_ustores/web/product_detail.jsp?PRODUCTID=95`

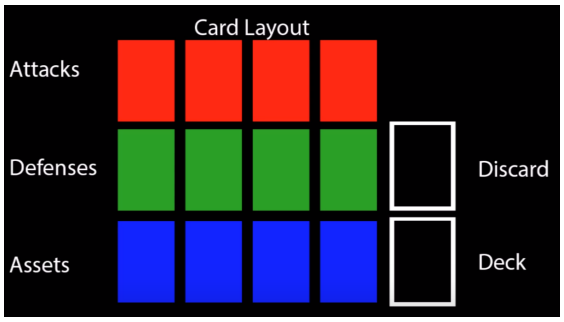


Figure 2.23: Cyber Threat Defender Game Card Layout (Thomas et al., 2019; CIAS, 2021).

Each player then shuffles their deck of cards and selects seven cards. Each player can play three cards and must discard cards if a player has more than five. It is an excellent strategy to place Defence Cards first, or another player can use Attack Card. For example, if you play Router Asset Card, then also play Encryption Card simultaneously. End of each turn, draw two more cards and discard if you have more than five. The first player to 30 points wins.

2.5.13 Exploit!

Description: Card game designed to teach players how to attack and defend servers. The game is available, and copies can be purchased[32] for approximately $23.99 (excluding postage correct as of 10/01/2022).

Number of Players: 2-4

Players Age: 12+

Brief Description of Gameplay
Quote "The game focuses on around how cyber attacks are developed. Each player has a set of target servers protected by a firewall that slowly grows vulnerabilities over time. You will spend your resources examining your opponent's firewall as well as cleaning your own. Then, when you find a critical vulnerability, you can exploit it and deliver a payload to steal data, vandalize websites, create botnets, and most importantly, score points!"

2.5.14 Operation Digital Chameleon

Description: The game aims (Rieb and Lechner, 2016) to train IT security professionals to deal with Advanced Persistent Threats (APTs).

Number of Players: 2-6 Players

Brief Description of Gameplay
The game board represents the critical IT infrastructure, three teams (each has a captain):

[32] https://www.thegamecrafter.com/games/exploits-a-hacker-s-card-game1

- Red Team – Attacks the infrastructure
- Blue Team – Security Defenders
- White Team – Moderates the play (Games Master, can include observers)

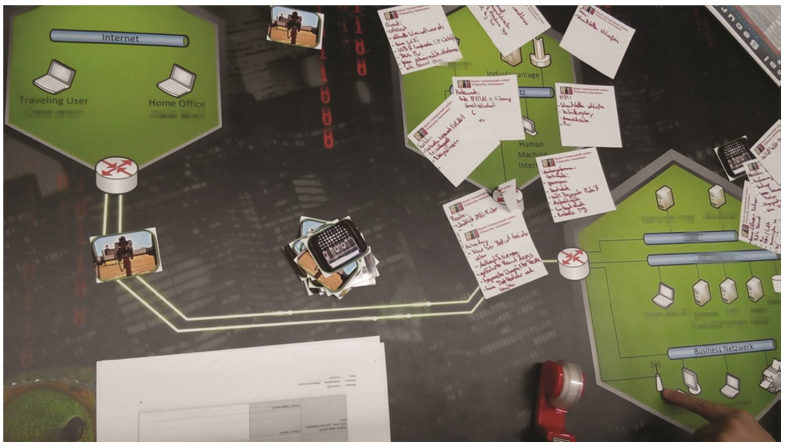


Figure 2.24: Operation Digital Chameleon Game Board (Rieb and Lechner, 2016).

The red team selects one of five threat actors, Nation States, Script Kiddies, Hacktivists, Employees, and Cyber Criminals, each with its own profile. The red team must stay within the plausible attack based on threat actor, so if an actor is Script Kiddies cannot be a zero-day exploit. The red team are encouraged to use attack trees. Teams are established by lottery. See Figure 2.24 Operation Digital Chameleon Game Board.

2.5.15 StixITS

Description: Structured Threat Information Expression (STIX™) (OASIS, 2019) is a language and serialisation format used to exchange cyber threat intelligence. StixITS was created to teach STIX concepts.

Brief Description of Gameplay
STIX, was initially sponsored by the office of Cybersecurity and Communications within the United States Department of Homeland Security. STIX is open source and free to download and change. STIX is based on use cases and designed to exchange cyber threat intelligence.

Average threat intelligence is limited to a flat file, for example, IP address, hash values and domain names. STIX version 2.0 gives opportunities to exchange much richer information and temporal base, so an example could say at what point in the attack the IP address was used. STIX package can contain one or more STIX objects, see Figure 2.25.

Table 2.10 is an example of a package of a phishing attack using the package objects: Indicator and Observed Data.

Figure 2.25: STIX Game Package Objects (OASIS, 2019).

Table 2.10: STIX Game Package Example: Threat Intelligence on Phishing attack.

Package Objects	Description
	Package Indicator - This contains a pattern that can be used to detect suspicious or malicious cyber activity.
	Package Observed Data - Conveys information observed on a system or network (e.g., an IP address).

2.5.16 Social Engineering Requirements Game

Description: Social Engineering Requirements (Beckers and Pape, 2016) is a card game designed to teach players how to attack and defend servers.

Brief Description of Gameplay
Primary Audience - employees that work with computers and information assets. Secondary Audience - Administration staff.

Section 1 - Preparation Plan overview – this is based on the organisation fire escape plan, and this is based on the reasoning that it is readily available. The example in Figure 2.26 shows the fire-extinguishers, fire alarm buttons, and escape routes.

Section 2 - Playing players take the role of the attacker in the following phases:

1. Draw Human Behaviour Pattern Card
2. Draw Attack Scenario Card
3. Choose Attack Type
4. Brainstorming

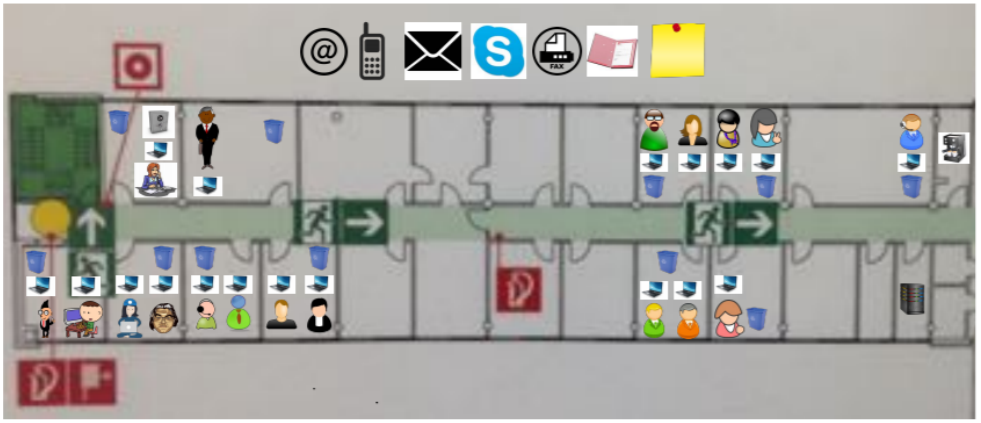


Figure 2.26: Social Engineering Requirements Game Board (Beckers and Pape, 2016).

5. Attack
6. Discussion

Section 3 – Debriefing The players reflect their attacks and may be supported by the company's security team.

2.5.17 Play2Prepare

Description: Play2Prepare (Graffer et al., 2015) is a tabletop board game similar to Pandemic (Z-Man Games, 2021), which simulates a significant scale attack on the electric power grid. The game consists of five scenarios and questions that are meant to trigger discussions and knowledge exchange. This board game intends to support organisations in strengthening their incident response capabilities.

Number of players: 3 to 4

Brief Description of Gameplay
Play2Prepare is a cooperative board game where the players will work together to mitigate attacks against the power grid network. The players let their pawns travel around the board to neutralise local attacks while the attack spreads in each round. Each player is assigned a particular role with accompanying skills that have to be utilised in the best possible manner to win the game.

Scenarios

- Scenario 1: Smart meters
- Scenario 2: Social manipulation and insider threats
- Scenario 3: A zero-day attack
- Scenario 4: Privacy and smart meters
- Scenario 5: Threats and the media

Game Board In the current version of Play2Prepare, the board, represents part of Norway's central power distribution network. The target players for the current version of the game are employees at Statnett, the organisation that manages the central power distribution network in Norway. The board can be changed.

Cards An attack will be mitigated when a player collects five Player cards with different numbers representing the five phases in the ISO/IEC 27035 information security incident management standards. The five phases in ISO/IEC 27035 are: 1) Plan and prepare 2) Detection and reporting 3) Assessment and Decision 4) Responses and 5) Evaluation and lessons learnt.

Game objective: Players collectively win the game immediately when three attacks have been mitigated.

2.5.18 The Security Cards

Description: The Security Cards (Tamara Denning, Batya Friedman, and Tadayoshi Kohno, 2021) was created to facilitate the exploration of potential security threats for a particular system, and more broadly, to help develop a security mindset. The game is available to purchase[33] a set of cards for approximately $19.00 (excluding postage correct as of 11/01/2022). The game is also available to download[34] under a creative commons 3.0 license for self-printing.

Audience Educators (for their students), Researchers, and Practising Professionals.

Cards 42 cards in 4 suits:

- Human Impact
- Adversary's Motivations
- Adversary's Resources
- Adversary's Methods

Note: Option to create custom cards

Step-by-Step Activities The Security Cards are used in an educational or training context

- Sorting by Threat Importance - Have participants consider a specific system. With that system in mind, ask participants to consider each dimension independently and sort the cards within that dimension to determine how relevant and risky it is for the system overall.
- Multi-Dimensions of Threat Discovery - Have participants consider a specific system. With that system in mind and using the entire card deck, have participants explore card combinations from different dimensions to surface possible threats to the system.

[33] https://www.ubookstore.com/The-Security-Cards
[34] https://securitycards.cs.washington.edu/

2.5.19 Crypto Go

Description: Crypto Go, a physical card game that may be used both as dissemination and educational tool (González-Tablas et al., 2020) for teaching cryptography. The game is available to download from the Crypto Go Website[35] and self-printing[36].

Audience: Students enrolled in STEM degrees. However, the "*...first prototype aiming at a flexible tool that could be adapted to serve as an instructional game in a wide variety of environments, and be useful for boosting motivation in individuals with poor (or even non-existent) prior knowledge in the field..*".

Cards 108 cards in 6 different types of cryptographic tools:

- stream ciphers (SCs) - colour red
- block ciphers (BCs) - colour pink
- hash functions (Hs) - colour orange
- operation modes (OMs) - colour yellow
- authenticated encryption modes (AEs) - colour green
- message authentication codes (MACs) - colour blue

Figure 2.27: Crypto Go Game Card Sample of Crypto Kit Types and Cheat Cards (González-Tablas et al., 2020).

In addition, players are given two cheat cards that explain how these tools interplay to derive a secure cryptographic construction (see Figure 2.27).

Brief Description of Gameplay

The goal of each player is to form as many Crypto Kits as possible (see Figure 2.28).

A Crypto Kit is a card set representing cryptographic tools that suffice to attain the three main qualities targeted in symmetric cryptography is 1) Confidentiality, which is used to make sure that nobody can read what data or information is sent between the two parties), 2) Integrity, which is used to ensure that nobody in between can change some parts of the shared information, and 3) Authentication, which is used to make sure that you communicate with the person you want to.

[35] https://www.cryptogogame.com/ES
[36] https://e-archivo.uc3m.es/handle/10016/28433

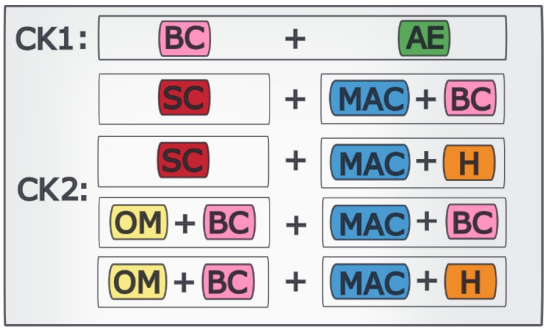


Figure 2.28: Crypto Go Game Summary of Crypto Kits (González-Tablas et al., 2020).

Players are dealt six cards and select one and place this face down in front of them. They then each pass their hand of cards to the person on the left. The gameplay continues until players have one card, and then each player takes four cards from the main deck. Furthermore, each player may use the cards in their hand to replace up to two of their already played cards, discarding the cards that have been substituted in a face-down pile on the table. Now, game direction shifts by players passing cards to the right. When there are no cards left to pass and each player has collected ten cards, the round ends and scores are publicly computed. Players score 16 points for each completed Crypto Kit. The player with the highest score after three rounds wins the game.

2.5.20 LINDDUN GO

Description: LINDDUN is a privacy threat modelling framework that provides support to elicit systematically and mitigate privacy threats in software architectures, and it was based on the Microsoft STRIDE threat model (Wuyts et al., 2020). LINDDUN GO game is a trimmed-down variant of LINDDUN that helps teams look at their software design from a privacy perspective to identify potential threats. The LINDDUN GO game is available online[37] or to purchase a set of cards for approximately £15.99 (excluding postage correct as of 12/12/2021). Players first create a Data Flow Diagram (DFD) and then use the cards to elicit privacy security threats.

Audience: A team, including a domain expert, system architect, developer, DPO, legal expert, CISO, privacy champion.

Cards The cards represent the 34 of the most common privacy threats and are designed to guide the players through the threat analysis process. They come in six suits matching six of seven **LIND**(Ð)**UN** privacy threat categories. Excludes **D**etectability: You can distinguish whether an item of interest exists or not.

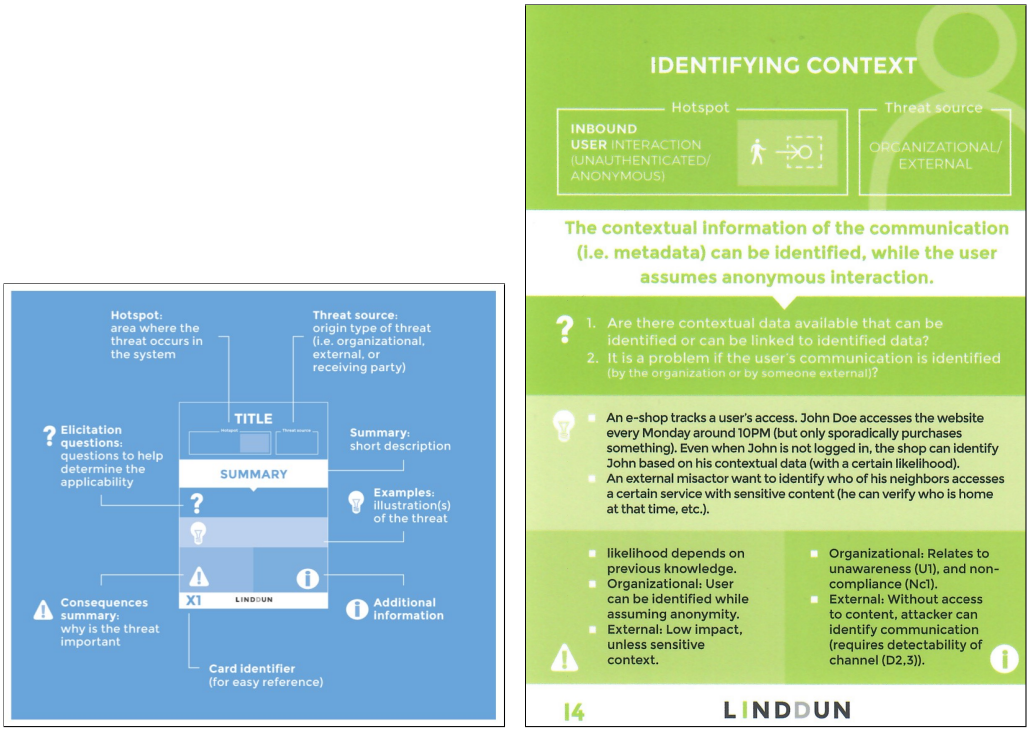
Six privacy threat categories: **L**inkability: You can distinguish whether two items are linked, even without knowing the identity of the subject. **I**dentifiability: You can identify the subject within a set of subjects. **N**on-Repudiation: A data subject cannot deny they know, did, said something. **U**nawareness: A data subject is unaware of, or unable to intervene in, the collection and

[37] https://www.linddun.org/go

processing of their personal data. **D**isclosure of information: An adversary can learn the content of an item of interest about a data subject. **N**on-Compliance: The system does not comply with data protection principles.

Brief Description of Gameplay

1. Gather a group of threat modelling enthusiasts (2 to 5 participants), see audience
2. Have or create a model of the system (a Data Flow Diagram (DFD) model is preferred)
3. Model must contain at least elements that correspond to the hotspot types used by LINDDUN GO game (see Figure 2.29 for example of threat card elements, "Hotspot"):
   - Inbound Communication
   - Outbound Communication
   - Processes
   - Storage and Retrieval Actions
4. Assign a secretary that will document the threats
5. Shuffle the Threat Cards and make 1 Draw Pile
6. The first threat modeller draws a card from the Draw Pile and tries to identify an applicable threat
7. Document threat if found by player who drew the card
8. Take turns to find all threats related to the card and document
9. Put card in discard pile and next player draws a card



(a) Threat Card Summary (b) Example Threat Card - **L**inkability

Figure 2.29: LINDDUN GO Threat Card Example (Wuyts et al., 2020).

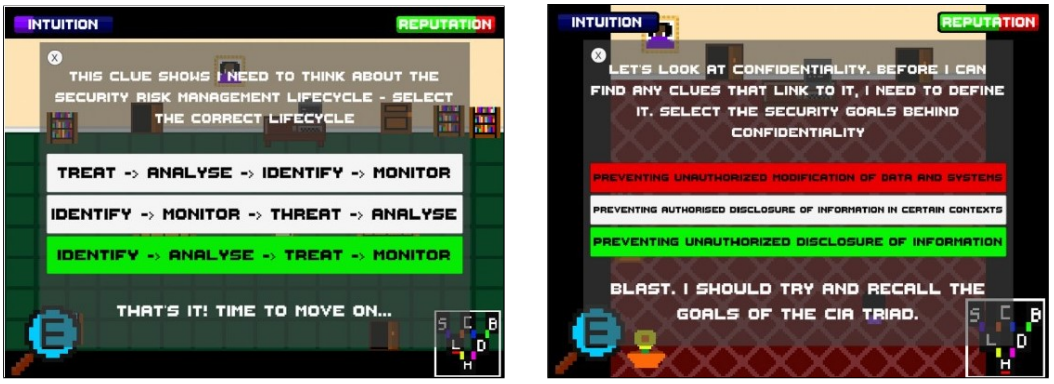
2.5.21 SherLOCKED

Description: SherLOCKED is a multi-level, top-down 2D detective-themed game that involves the player assuming the role of a detective navigating through a house (Jaffray et al., 2021). The game was designed using the Unity game engine[38] to support students remote learning during the Covid-19 pandemic. The game questions dictate how players progress. These questions have been created using lecture content from the first half of an introductory cyber security module. The game is designed to support remote learning so players can build on knowledge. Jaffray et al. noted that there was significant difficulty finding the motivation to watch lecture recordings and attend live online sessions. SherLOCKED was designed to support students using gamification principles to create engagement following feedback from internal student consultations.

Audience: SherLOCKED, targeted at undergraduate computer science university students.

Brief Description of Gameplay

The players act the role of cyber investigator after the attack and a defender through three case studies. In the first case study, the detective meets the victim and looks for clues through the hacked home. In the second case study, the player is in the computer room. Here, they try to learn more about the hacker's targeting. The third case study involves the player acting as the detective walking around the various rooms to secure the house from the risk of future hacking. Similar to the educational context the game provides feedback if the question is correct or incorrect, see Figure 2.30.



(a) Correct answer with praise and Intuition points given

(b) Incorrect answer with feedback and Reputation points lost

Figure 2.30: SherLOCKED feedback on player selection (Jaffray et al., 2021).

[38] https://unity.com/solutions/game

2.5.22 GAP: A Game for Improving Awareness About Passwords

Description: An online game designed to educate users about the following six insecure password creation strategies (Tupsamudre et al., 2018).

1. use of capital letters at the beginning of the password
2. use of only capital letters in the password
3. use of digits at the beginning of the password
4. use of digits at the end of the password
5. use of symbols at the beginning of the password
6. use of symbols at the end of the password

Audience: Educate users about various features that negatively impact password security.

Brief Description of Gameplay

The goal of the player is to exit the maze by destroying all six barriers (insecure passwords) along the path, see Figure 2.31. The movement of the tank is controlled using left and right arrow keys and the movement of the turret is controlled using the mouse. There are three types of ammunitions out of which the player has to choose the right one depending on the password label of the barrier. If wrong ammunition is fired, the health of the tank decreases and the barrier remains unaffected. In short, the game requires the player to look at the password label (princess1), identify insecure operation (digit at the end) and choose the right ammunition (key D) to destroy the barrier.

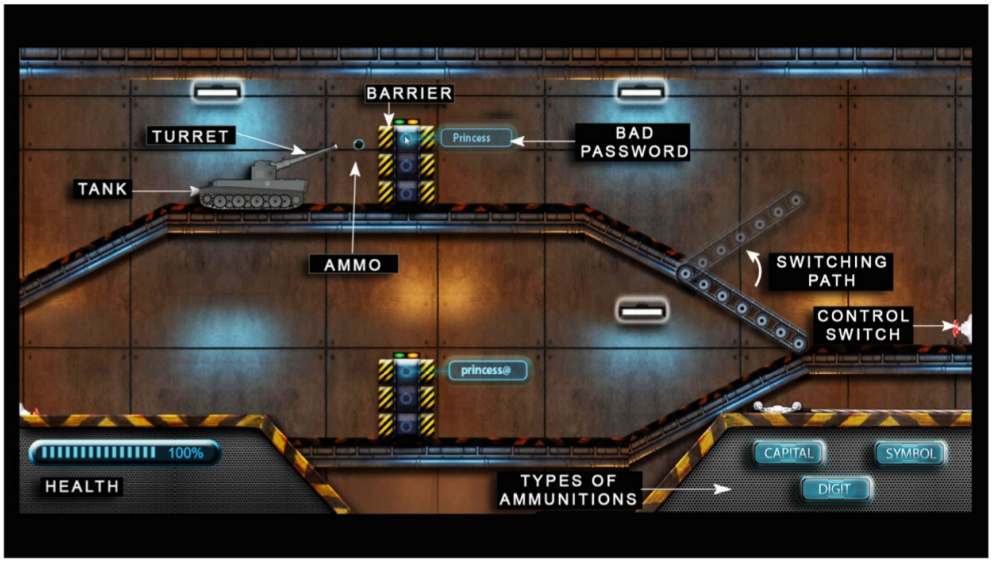


Figure 2.31: The interface of GAP, a web-based game to educate players about insecure password creation strategies (Tupsamudre et al., 2018).

2.6 Summary of Games

Table 2.11 is a summary of the games detailed in Section 2.5. Fourteen games have the player attacking only. Nine games have players defending only, with just six of the nineteen games attacking and defending. One speciality game, StixITS, does not have the concept of attacking or defending. All of the game scenarios are very limited.

Table 2.11: Summary of Serious Security Games

No	Game	Game Scenarios	Gameplay Attacking	Gameplay Defending	Brief Description
2.5.1	Elevation of Privilege	Application development	Yes	No	Card game for threat modelling using Microsoft STRIDE.
2.5.2	OWASP Cornucopia	Application development	Yes	No	Same as EoP but based on OWASP Secure Coding Practices.
2.5.3	Protection Poker	Database design	Yes	No	Calculate the most vulnerable & valuable tables in the database.
2.5.4	Hacker	Software Coding	Yes	No	Out the box game to teach secure coding.
2.5.5	CyberCIEGE	Office environment	No	Yes	Interactive educational video game.
2.5.6	PERSUADED	Social Engineering	Yes	Yes	Computer game to teach how to protect from attacks.
2.5.7	Cyber Security Requirements Awareness Game	Hospital related scenarios	Yes	No	Tabletop game to teach risks in hospital scenarios.
2.5.8	Decision & Disruption	Utility Company	No	Yes	The game board is based on Lego. Players must prioritise defences to given budget.
2.5.9	Control-Alt-Hack	White Hack Hacker	Yes	No	A card game where you compete against other players.

Continued on next page

Table 2.11 – continued from previous page

No	Game	Game Scenarios	Gameplay Attacking	Gameplay Defending	Brief Description
2.5.10	[dox3d!]	Network Security	Yes	No	Tile-based game to create random network used by players to hack.
2.5.11	Cryptomancer RPG	Role-Play Game	Yes	Yes	Play game and has no restrictions on the gameplay.
2.5.12	Cyber Threat Defender	Defending & Protecting Assets	Yes	Yes	A two-player card game where they try to attack the other player whilst defending from attacks.
2.5.13	Exploit!	Attack & Defend Servers	Yes	Yes	Card game on attacking servers.
2.5.14	Operation Digital Chameleon	Advanced Persistent Threats (APTs)	Yes	Yes	Simulation of Red Team and Blue Team attack and defence.
2.5.15	StixITS	Exchange Cyber Threat Intelligence	No	No	Teach the use of structured threat information sharing based on STIX™ standard
2.5.16	Social Engineering Requirements Game	Attack & Defend Servers	Yes	Yes	Board Game for Eliciting Social Engineering Security Requirements.
2.5.17	Play2Prepare	Industrial Control Organisations	No	Yes	Support organisations in strengthening their incident response capabilities.

Continued on next page

Table 2.11 – continued from previous page

No	Game	Game Scenarios	Gameplay Attacking	Gameplay Defending	Brief Description
2.5.18	The Security Cards	In a wide range of contexts	Yes	No	Encourage you to think broadly and creatively about computer security threats.
2.5.19	Crypto Go	Cryptographic tools	No	Yes	Understanding how essential cryptographic tools work and interplay.
2.5.20	LINDDUN GO	Application development	Yes	No	Card game for privacy threat modelling using LINDDUN threat model
2.5.21	SherLOCKED	Cryptographic tools	No	Yes	Developed as part of an undergraduate course
2.5.22	GAP: A Game for Improving Awareness About Passwords	Identify weak passwords	No	No	Explore the potential of serious games to educate users about various features that negatively impact password security

2.6.1 Serious Games: by Category

Table 2.12 summarises the games detailed in Section 2.5 by categories: *Secure Software Development* (six games) and *Security Awareness and Education* (sixteen games).

Table 2.12: Serious Games: by Category.

Games	Category & Description
2.5.1 Elevation of Privilege 2.5.2 OWASP Cornucopia 2.5.3 Protection Poker 2.5.4 Hacker 2.5.16 Social Engineering Requirements Game 2.5.20 LINDDUN GO	**Secure Software Development** - Serious games created to support activities in software development
2.5.5 CyberCIEGE 2.5.6 PERSUADED 2.5.7 Cyber Security Requirements Awareness Game 2.5.8 Decisions & Disruptions 2.5.9 Control-Alt-Hack 2.5.10 [Dox3d!] 2.5.11 Cryptomancer 2.5.12 Cyber Threat Defender 2.5.13 Exploit! 2.5.14 Operation Digital Chameleon 2.5.15 StixITS 2.5.17 Play2Prepare 2.5.18 The Security Cards 2.5.19 Crypto Go 2.5.21 SherLOCKED 2.5.22 GAP: A Game for Improving Awareness About Passwords	**Security Awareness and Education** - Serious games used as means for security awareness and education

2.6.2 Serious Games: by Type

Table 2.13 is a summary of the games detailed in Section 2.5 by game types. Nine are card-based games, and seven are board based games with only four computer games. There were two games in particular categories, Cryptomancer which is a full Role Play Game (RPG), using six-sided and ten-sided dice and StixITS game, a speciality game for teaching methodology to exchange cyber threat intelligence.

Table 2.13: Serious Games: by Type.

Games	Type
2.5.1 Elevation of Privilege (Game Board Data Flow Diagrams) 2.5.2 OWASP Cornucopia (Game Board Data Flow Diagrams) 2.5.3 Protection Poker 2.5.9 Control-Alt-Hack (No game board but requires dice) 2.5.12 Cyber Threat Defender (No game board) 2.5.13 Exploit! (No game board) 2.5.18 The Security Cards 2.5.19 Crypto Go 2.5.20 LINDDUN GO	Card Games
2.5.5 CyberCIEGE 2.5.6 PERSUADED 2.5.21 SherLOCKED 2.5.22 GAP: A Game for Improving Awareness About Passwords	Computer Games
2.5.4 Hacker 2.5.7 Cyber Security Requirements Awareness Game 2.5.8 Decisions & Disruptions 2.5.10 [Dox3d!] 2.5.14 Operation Digital Chameleon 2.5.16 Social Engineering Requirements Game 2.5.17 Play2Prepare	Board Games (requires a unique game board to play)
2.5.11 Cryptomancer 2.5.15 StixITS	Other Games

2.6.3 Serious Games: with Defending

Table 2.14 summarises the games detailed in Section 2.5 that the player has a defending role in the gameplay. Eleven games have players defending in gameplay. Ten games only have players attacking in gameplay, with one speciality game, StixITS, which does not have the concept of attacking or defending.

Table 2.14: Serious Games: Have Defending.

Games	Defending
2.5.5 CyberCIEGE	Yes - Within budget to defend IT within the office environment
2.5.6 PERSUADED	Yes - Only for social engineering attacks
2.5.8 Decisions & Disruptions	Yes - Limited to defence utility company
2.5.11 Cryptomancer	Yes - As a role-playing game
2.5.12 Cyber Threat Defender	Yes - Two player game attacking and defending each other's assets
2.5.13 Exploit!	Yes - Defending servers through firewall
2.5.14 Operation Digital Chameleon	Yes - Against Advanced Persistent Threat actors
2.5.16 Social Engineering Requirements Game	Yes - Social engineering attacks on servers in an office context
2.5.17 Play2Prepare	Yes - Defending industrial control systems
2.5.19 Crypto Go	Yes - Cryptographic tools
2.5.21 SherLOCKED	Yes - Defending a house
2.5.1 Elevation of Privilege	No - Attacking only
2.5.2 OWASP Cornucopia	No - Attacking only
2.5.3 Protection Poker	No - Only mitigation to vulnerable database tables
2.5.4 Hacker	No - Only fixing program code
2.5.7 Cyber Security Requirements Awareness Game	No - Undercover Health IT team acting as attackers only
2.5.9 Control-Alt-Hack	No - Players act as white hat hackers
2.5.10 [Dox3d!]	No - Players act as white hat hackers to hack the systems to get data back
2.5.18 The Security Cards	No - To surface threats in system design and by project teams to communicate about potential security threats with management and others
2.5.20 LINDDUN GO	No - Attacking only
2.5.22 GAP: A Game for Improving Awareness About Passwords	No - Attacking only to find weak passwords
2.5.15 StixITS	No - About sharing threat intelligence, not defending or attacking

2.6.4 Serious Games: Target Audience

Table 2.15 is a summary of the games detailed in Section 2.5 by the target audience. Some of the games explicitly state the target audience for the game, and some were identified by analysis of the gameplay. All the games have a bias targeting employees (five games) or technical/professional employees or students (fifteen games). Only one game Control-Alt-Hack has targets more than one group of players.

Table 2.15: Serious Games: Target Audience.

Game	Software Developers	Database Developers	Technical Teams	Employees Organisation	High School Students	University STEM Students	Security / Privacy Professionals
2.5.1 Elevation of Privilege	X						X
2.5.2 OWASP Cornucopia	X						
2.5.3 Protection Poker		X					
2.5.4 Hacker					X		
2.5.5 CyberCIEGE				X			
2.5.6 PERSUADED				X			
2.5.7 Cyber Security Requirements Awareness Game				X			
2.5.8 Decisions & Disruptions				X			X
2.5.9 Control-Alt-Hack					X	X	
2.5.10 [Dox3d!]						X	
2.5.11 Cryptomancer						X	
2.5.12 Cyber Threat Defender			X				
2.5.13 Exploit!			X				
2.5.14 Operation Digital Chameleon							X
2.5.15 StixITS			X				
2.5.16 Social Engineering Requirements Game			X				X
2.5.17 Play2Prepare				X			
2.5.18 The Security Cards					X		X
2.5.19 Crypto Go						X	
2.5.20 LINDDUN GO	X						X
2.5.21 SherLOCKED						X	
2.5.22 GAP: A Game for Improving Awareness About Passwords	X	X	X	X	X	X	X
Count	**4**	**2**	**5**	**6**	**4**	**6**	**7**

2.6.5 Serious Games: Player Game Roles

Table 2.16 is a summary of the games detailed in Section 2.5 by game player role. The player plays a defined role in all the games, for example, the attacker/hacker, defender or red team member. Only one game Cryptomancer allows the player to select their role.

Table 2.16: Serious Games: Player Game Roles.

Games	Attacking Role	Defending Role
2.5.1 Elevation of Privilege	Software developer	n/a
2.5.2 OWASP Cornucopia	Software developer	n/a
2.5.3 Protection Poker	Database Administrator	n/a
2.5.4 Hacker	Hacker	n/a
2.5.5 CyberCIEGE	n/a	IT Manager
2.5.6 PERSUADED	Attacker (Generic)	Defender (Generic)
2.5.7 Cyber Security Requirements Awareness Game	Network Attacker or Social Engineering Attacker or Physical Attacker	n/a
2.5.8 Decisions & Disruptions	n/a	Defender (Generic)
2.5.9 Control-Alt-Hack	White hat hacker	n/a
2.5.10 [Dox3d!]	Attacker (to recover your lost data)	n/a
2.5.11 Cryptomancer	Play any role	Play any Role
2.5.12 Cyber Threat Defender	Attack another player	Defend from another player
2.5.13 Exploit!	Attack another player	Defend from another player
2.5.14 Operation Digital Chameleon	Red Team	Blue Team (also white team to moderate)
2.5.15 StixITS	n/a	n/a
2.5.16 Social Engineering Requirements Game	IT Social Engineering Attacker	Administrators
2.5.17 Play2Prepare	n/a	Assigned a role (6 role cards)
2.5.18 The Security Cards	Adversary: Motivations; Resources; and Methods	Sorting by Threat Importance
2.5.19 Crypto Go	n/a	Collecting sets of cards that represent solid cryptographic constructions
2.5.20 LINDDUN GO	Play any role	n/a
2.5.21 SherLOCKED	Cyber Investigator (Professional)	Cyber Investigator (Professional)
2.5.22 GAP: A Game for Improving Awareness About Passwords	Find weak passwords	n/a

2.7 Brief summary of each cyber game

The following briefly describes each of the security games found for review (more information, see Section 2.5):

Elevation of Privilege (EoP) is a card game based on the Microsoft STRIDE threat model. It was designed for technical staff to review and find vulnerabilities in data flow diagrams they created during the software development cycle. The players act as attackers and win points for valid attacks. The player with the highest points wins.

OWASP Cornucopia is a tabletop card game designed like the Elevation of Privilege (EoP). The game is played by technical staff during the software development cycle to elicit vulnerabilities during the software development cycle. Instead of Microsoft STRIDE the cards, it uses The Open Web Application Security Project (OWASP): secure coding practices, application security, and testing guide.

Protection Poker is a tabletop card game based on a hypothetical health system database. The gameplay is not about winning but calculating the risk of the functions in the database and then ranking them.

Hacker is a tabletop game focusing on secure coding practices. The game features several coding challenges of increasing difficulty that aims to educate how to code vulnerabilities that can be discovered, exploited and protected.

CyberCIEGE 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.

PERSUADED game allows players to learn the effectiveness of defence controls against most common social engineering attacks. Still, it does not raise awareness of the actual attack vectors that attackers can exploit.

Cyber Security Requirements Awareness Game is a tabletop card game developed to educate players about cyber security risks in hospital-related scenarios. For advanced users, they need not to use the already designed map. They can generate any hypothetical map of their own by using the assets cards.

Decision & Disruptions is a tabletop game and is very visual, using Lego as the game board. Players act as defenders of a small utility company with two locations. Players must manage security within a given budget. The gameplay has an element of surprise at the end of the game the games master reveals all the attacks and which ones they defended and successful attacks, which they did not defend against

Control-Alt-Hack is a tabletop card game where players act as hackers, and the game objective is to gain enough hacker points to become the CEO or retire.

[Dox3d!] is a team tabletop card game, and bad guys have stolen your data. As a group, you must hack the network and get your data back. All players must escape and meet at the internet gateway, and if you do not all escape, you are '[Dox3d!]' and lose.

Cryptomancer RPG is a tabletop role-playing game, and the gameplay could go in any direction by the games master. The instructions are 440 pages long, and the game is a very complex game to understand.

Cyber Threat Defender is a tabletop card game based on assets, defences and attack cards that are very easy to understand. Players act as attackers and defenders and learn it is an excellent strategy to play defence cards first. The first player to 30 points wins.

Exploit! is a tabletop card game to teach players how to attack and defend servers. Players review the opponent's firewall whilst reviewing the security on their firewall. The task is to find a vulnerability in the opponent's firewall and exploit it to score points.

Operation Digital Chameleon is a tabletop card game is specially designed to teach security professionals to deal with APT. The gameplay has three teams: Red Team, as the attackers; Blue Team, as the Defenders; and White Team, as the game moderators. The Red Team must use a plausible attack from an attack actor.

StixITS Structured Threat Information Expression (STIX™) was initially sponsored by the office of Cyber Security and Communications within the United States Department of Homeland Security. STIX is based on use cases and designed to exchange cyber threat intelligence. The game is designed to teach the player how to use the STIX methodology to exchange threat intelligence.

Social Engineering Requirements Game is a tabletop card game designed to teach players to attack and defend servers. The gameplay uses the organisation fire escape plan. The main goal is to provide structured means to elicit and prioritise social engineering security requirements. The game is designed for any employee, and the player with the highest points wins.

Play2Prepare is a tabletop board game with five scenarios whose primary goal is to train players in preparedness exercises to handle IT security incidents in Industrial Control Organisations. The players must complete five phases of International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27035 information security incident management standards to defend from the attack. Players win after defending from three attacks.

The Security Cards is a card game 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 kinds of educational activities in academic and industry settings.

Crypto Go is a card game where the goal of each player is to form as many Crypto Kits as possible. For instance, a Crypto Kit can consist of an SC card (stream ciphers), a MAC card (message authentication codes), and either a BC (block ciphers) or an H card (hash functions).

LINDDUN GO is a card game where the goal of each player is to find privacy threats using the LINDDUN threat model, based on a Data Flow Diagram the players have created.

SherLOCKED is a computer 2D detective-themed game that involves the player assuming the role of a detective navigating through a house. It is designed to support University students on a cyber course. Players act as an investigators to find why the house was breached and recommend changes to prevent future breaches.

GAP: A Game for Improving Awareness About Passwords is a computer game that involves the player moving around a maze in a tank to get past barrier by identifying and attacking part of the weak password.

2.8 Criteria to select games for further review

Table 2.17 lists the nineteen games identified for review and put through to the next step to be compared using the criteria listed below:

1. **Availability** - The availability criteria are based on whether the game is freely available. It will have limited take up if organisations must pay to view the game for suitability. Several games in academic studies cannot be found in a product search and raise questions on suitability (Hendrix et al., 2016). However, if the game is available to purchase from a known source online, the game was purchased for review, such as Microsoft EoP 2.5.1.
2. **Speciality Games** - Some of the games have specific target groups. For example, Control-Alt-Hack is designed for players to act as White Hat Hackers (see subsection 2.5.9). Games were only excluded if not designed for awareness and education or role-based games designed specifically for gamers. For example, Cryptomancer, see subsection 2.5.11, which is only suitable for experienced RPG players.

Table 2.17: Potential Serious Games to be Reviewed.

Game	Reviewed	Further Investigation	Reason for Rejection
Elevation of Privilege see subsection 2.5.1	Yes	Yes	
OWASP Cornucopia, see subsection 2.5.2	Yes	Yes	
Protection Poker, see subsection 2.5.3	Yes	Yes	
Hacker, see subsection 2.5.4	Yes	Yes	
CyberCIEGE, see subsection 2.5.5	Yes	Yes	
PERSUADED, see subsection 2.5.6	Yes	Yes	
Cyber Security Requirements Awareness Game, see subsection 2.5.7	Yes	Yes	
Decisions & Disruptions, see subsection 2.5.8	Yes	Yes	
Control-Alt-Hack, see subsection 2.5.9	Yes	No	Cost approx. $30.00 but unable to get a copy of the cards at review time
[dox3d!] see subsection 2.5.10	Yes	Yes	
Cryptomancer RPG, see subsection 2.5.11	Yes	No	Only suitable for experienced RPG players, instructions run to 440 pages
Cyber Threat Defender, see subsection 2.5.12	Yes	Yes	
Exploit!, see subsection 2.5.13	No	No	Cost approx. $23.99 but unable to get a copy of the cards at review time
Operation Digital Chameleon, see subsection 2.5.14	Yes	No	Game not available
StixITS, see subsection 2.5.15	Yes	No	Stix is used to share Threat intelligence

Continued on next page

Table 2.17 – continued from previous page

Game	Reviewed	Further Investigation	Reason for Rejection
Social Engineering Requirements Game, see subsection 2.5.16	Yes	Yes	
Play2Prepare, see subsection 2.5.17	Yes	Yes	
The Security Cards, see subsection 2.5.18	Yes	Yes	
Crypto Go, see subsection 2.5.19	Yes	No	Very targeted game for STEM students on cryptography sets
LINDDUN GO, see subsection 2.5.20	Yes	Yes	
SherLOCKED, see subsection 2.5.21	Yes	Yes	
2.5.22 GAP: A Game for Improving Awareness About Passwords	Yes	No	Interesting gameplay and feedback, but only used for password security

2.9 Comparison of cyber games selected

Fifteen games were selected for further investigation, see Table 2.18, based on the criteria in Section 2.8, from the original nineteen games in Table 2.17.

Table 2.18: Comparison of Serious Games.

Game	Game Adaptable	Game Objective	Target Audience	Background Players
Elevation of Privilege, see section 2.5.1	Yes Creative Comms License	Identify vulnerabilities in data flow diagrams whilst in software development	Software development teams	Technical team proficient with data flow diagrams and technology
OWASP Cornucopia, see section 2.5.2	No	Identify vulnerabilities in data flow diagrams whilst in software development	Software development teams	Technical team proficient with data flow diagrams and technology
Protection Poker, see section 2.5.3	No	Identify and calculate the risks	Software development teams	Technical team proficient with data flow diagrams and technology
Hacker, see section 2.5.4	No	Identify and fix vulnerabilities in code	Students	No coding skills required has game board and book of examples and answers
CyberCIEGE, see section 2.5.5	No	Office scenarios players must invest limited budget to defend from attacks	Agencies of US Government	Requires understanding of VPN, Network Equipment and Encryption as in game have budget to buy and configure defences

Continued on next page

Table 2.18 – continued from previous page

Game	Game Adaptable	Game Objective	Target Audience	Background Players
PERSUADED, see section 2.5.6	No	Learn controls against most common social engineering attacks	Company Employees	Computer based game and players can learn social engineering attacks and best defence through the gameplay
Cyber Security Requirements Awareness Game, see section 2.5.7	No	Educate cyber risks in hospital scenarios	Hospital employees	
Decisions & Disruptions, see section 2.5.8	Yes Creative Comms License	To protect critical infrastructure of small utility company from attack	Stakeholders making security decisions	Players require no preparation to play
[dox3d!], see section 2.5.10	Yes Open Source	Designed teach students network security	Ethical hackers Network security staff	University Students Networking Security
Cyber Threat Defender, see section 2.5.12	No	To teach middle school students cyber vocabulary or high school students understanding of defence implementations	Players 11+	Engaging game regardless of age or skill level of players in cyber security
Social Engineering Requirements Game, see section 2.5.16	Yes	Based on the players organisation fire escape plan, the players attack and defend servers	Employees Organisation	No background Security Required

Continued on next page

Table 2.18 – continued from previous page

Game	Game Adaptable	Game Objective	Target Audience	Background Players
Play2Prepare, see section 2.5.17	Yes	Facilitates knowledge exchange and awareness raising through a set of scenarios	Employees Organisation	No background Security Required
The Security Cards, see section 2.5.18	Yes	Learn about security threats & training software and hardware developers	Students & Employees Organisation	No background Security Required
LINDDUN GO, see section 2.5.20	Yes	Elicit privacy security threats	Students	Organisation employees involved with privacy issues
SherLOCKED, see section 2.5.21	No	Support University Students in a Cyber Course	Students	On University Course linked to the game

2.10 Experience security decision-makers

The majority of the games reviewed assume knowledge in the players in technical security, for example, OWASP Cornucopia (Thompson and Takabi, 2016), designed to assist software development teams. The Social Engineering Requirements game (Beckers and Pape, 2016) tries to elicit vulnerabilities created by the personal behaviours of individual employees. Although the primary target group was security engineers and IT administrators, it identified the second group as the administration staff. Some games limit the vulnerabilities to a specific technology. For example, protection poker goes through a process to identify the most critical tables in a database. None of the games is designed for executives making the final investment decisions on security controls to protect the organisation. However, The Social Engineering Requirements game (Beckers and Pape, 2016) identified the need for "context-specific" threats to the organisation and used the office fire escape plan as a game board.

2.11 Use of games for learning security and awareness

One of the most significant decisions facing organisations is how much to spend on Information / Cyber Security. Senior executives must make decisions on investments of defences to mitigate against vulnerabilities they do not understand. (Holdsworth and Apeh, 2017) propose using gamification to create an immersive and effective Cyber Security Awareness program. Holdsworth and Apeh (2017) approach align the needs of the business against the needs of the individual and, as such, identifies in the hospitality sector the area of research three groups: Strategic, Tactical, and Operational. The game for each group may be different as it requires different learning outcomes.

2.11.1 The time that is taken to learn security game

For games that require a games master, an important part and key to all these games are how good the games master is at explaining the gameplay and keeping the play going. The games that require a games master, it is essential that they know the cyber expertise in the area the game covers. If the game does not require a games master, the design needs to ensure that the game does not require considerable time learning. For example, even with a game master, the instructions for Cryptomancer (Cryptomancer RPG, 2018) are 440 pages and were excluded from the literature review.

2.11.2 Games learning outcomes

The games in Table 2.19 have different objectives and learning outcomes. There is bias in the games that the majority focus on identifying vulnerabilities. In only two games, the players must propose mitigation or play mitigation card, Cyber Threat Defender subsection 2.5.12 and Decisions and Disruptions (DD) subsection 2.5.8, the game has a limited budget for defence.

A significant issue facing all organisations holding European Union (EU) citizen data is the new General Data Protection Regulation (GDPR) (European Union (EU), 2018), which entered into application on the 25 May 2018 (now replaced by UK Data Protection Act 2018). Majority of the games reviewed concentrate on security risks to data, except LINDDUN Go which concentrates on privacy threats. Three of the games considered privacy threats, Decisions & Disruptions (updated version), SherLOCKED, and EoP (see Figure 2.6).

Table 2.19: Games Learning Outcomes.

Game	Covers Security Issues	Covers Data Privacy	Player Role	Learning Outcomes Attack	Learning Outcomes Defence
Elevation of Privilege, see section 2.5.1	Yes	Yes	Act as hacker	In the context of the game board they created	Not covered in the game
OWASP Cornucopia, see section 2.5.2	Yes	No	Act as hacker	Yes	No
Protection Poker, see section 2.5.3	Yes	No	Act as hacker	Yes, it computes the threat as a score	Yes, add mitigations to high-risk processes (scored in-game)
Hacker, see section 2.5.4	Yes	No	White Hat Hacker then as a coder to defend	Yes, but only defence based on secure coding	Create secure code
CyberCIEGE, see section 2.5.5	Yes	No	Act as a defender to protect office IT infrastructure	Learn how to defend against attacks	Cost and configuration of defences
PERSUADED, see section 2.5.6	Yes	No	Act as a defender to protect against social engineering attacks	Only attacks that use social engineering	Only defences to social engineering attacks

Continued on next page

Table 2.19 – continued from previous page

Game	Covers Security Issues	Covers Data Privacy	Player Role	Learning Outcomes Attack	Learning Outcomes Defence
Cyber Security Requirements Awareness Game, see section 2.5.7	Yes	No	Team game act as either: network attacker; social engineer attacker; and third physical attacker	Yes, Attacks for networks, social engineering and physical attacks	Defences for networks, social engineering and physical attacks
Decisions & Disruptions, see section 2.5.8	Yes	Yes	Defender with a limited budget	Yes, based on the given scenario, not context-specific to organisation	Yes, limited to budget
[Dox3d!], see section 2.5.10	Yes	No	Act as a hacker to get your data back	Against network components	Although defence learning is not in gameplay, players learn how attacks traverse the network
Cyber Threat Defender, see section 2.5.12	Yes	No	Attacker and defender	Cards cover a wide range of attacks	Cards cover a wide range of defences
Social Engineering Requirements Game, see section 2.5.16	Yes	No	Act as hacker	Yes, from social engineering	No, whilst they learn about social engineering attacks, does not explicitly ask them for mitigations

Continued on next page

Table 2.19 – continued from previous page

Game	Covers Security Issues	Covers Data Privacy	Player Role	Learning Outcomes Attack	Learning Outcomes Defence
Play2Prepare, see section 2.5.17	Yes	No	Defined role with accompanying skills	Five Scenarios	Improved future defence from cyber attacks
The Security Cards, see section 2.5.18	Yes	No	Attacker	Cards cover a wide range of attacks	Which threats are most relevant overall, sorting threats by importance
LINDDUN GO, see section 2.5.20	No	Yes	Identify privacy threats	Find privacy issues to be resolved	n/a
SherLOCKED, see section 2.5.21	Yes	Yes	Attacker & Defender (Investigator) covers CIA triad	Related to University Course	Related to University Course

2.12 Gaps Identified in Current Serious Cyber Games

In the serious cyber games reviewed in this chapter, we identified several gaps:

Issue 1: The main issue found was that the individual games reviewed may achieve their stated learning objectives but do not define or link games mechanics or pedagogical theory to be adapted to achieve different learning objectives.

Issue 2: Games designed for a particular purpose and can't be changed, for example, Protection Poker for health system database (see subsection 2.5.3); Operation Digital Chameleon only for Advanced Persistent Threats (see subsection 2.5.14); and Decisions & Disruptions for a small utility company (see subsection 2.5.8).

Issue 3: Games designed for a player to act as attacker or defender very few games allow players to play both of the games learning outcomes (see Table 2.19) only three games have attacking and defending: Persuaded (see subsection 2.5.6); Cyber Threat Defender (see subsection 2.5.12); and Social Engineering Requirements Game (see subsection 2.5.7).

Issue 4: Games designed for technical (OWASP, see 2.5.2) or non-technical payers (Social Engineering Requirements Game see subsection 2.5.7) but cannot be adapted for both.

Issue 5: Some games are adaptable (see Table 2.18) but very limited, for example [Dox3d!], open-source but limited to network security, see subsection 2.5.10.

2.13 Conclusion a Pedagogical Design of New Game

The literature review identified several gaps in the currently available security games to meet the research aims and objectives. "Can one use a pedagogical design model to create a serious cyber game to teach cyber security awareness and education to meet organisational objectives? The games must be able to be played with technical and non-technical staff with no background in cyber security. Can the games also teach cyber security threats, vulnerabilities, defences and be adapted to organisational specific industry threats and vulnerabilities".

The literature review also noted that cyber games could also be used for risk management. An example is the Elevation of Privilege game (Microsoft, 2018; Shostack, 2014), used in the software development life cycle.

It is possible using a pedagogical approach to design a cyber game that can teach cyber security awareness and education and assist organisations risk management process in a dynamic changing landscape of new threats by a move to cloud services. Because cloud services bring new

threats and possible vulnerabilities, the design model needs to adapt to this to include changing landscape.

The five major components of constructivism defined by Driscoll (Driscoll, 2000) could be used to design and create curriculum content using constructivist principles that the content is designed to meet the learners' requirements in cyber security and education to promote high-level thinking skills and meet the game objectives.

Figure 2.32 identifies the areas that need to be considered for a pedagogical design for a serious game to teach cyber security and awareness. The key areas are **Serious Games** these are pedagogical theories used in serious games that can be applied to serious cyber games, for example, SDT. **Cyber Serious Games** is split into two areas. The first is essential to understand the serious intent and objectives. The second is the possible design elements unique or unique elements to serious cyber games, such as defences using NCSC guidance.

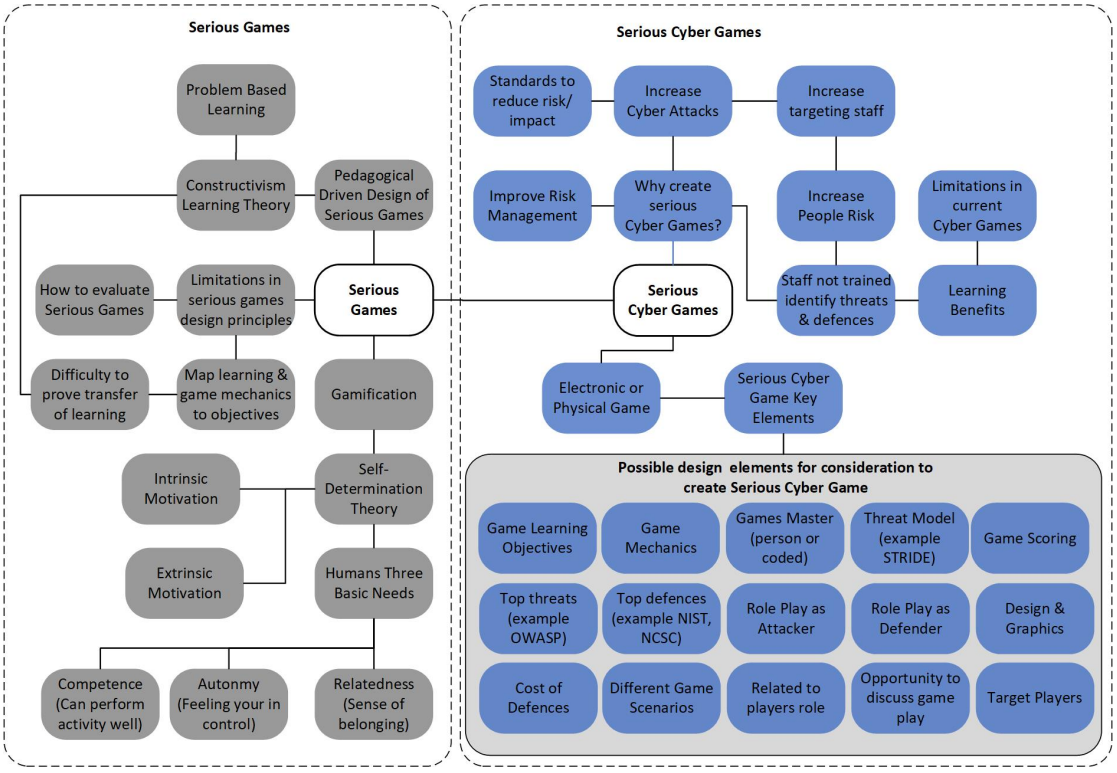


Figure 2.32: Serious Cyber Games Research Areas required for Consideration in a Pedagogical Design.

The key objectives, the pedagogical design linked to research aims and objectives (see Section 2.1) of the new serious cyber games design model needs to:

1. Ensure players' intrinsic and extrinsic motivation is considered in the design process, see Section 2.1 Gamification and Serious Games, (research aims and objective 5).

2. Use constructivism principles, for example, create five conditions for instruction in gameplay and game mechanics, see Section 2.2 Pedagogical Game Design (research aims and objective 5).

3. Game mechanics and play based on problem-based learning, see Figure 2.2 Model of Curriculum Shift to Problem Based Learning (Seng, 2000). (research aims and objective 3).

4. Ensure the game is based on a risk framework known and used in the industry the players are from, see Section 2.3 Methodologies for Risk Management (research aims and objective 4).

5. The new pedagogical design model must consider the taxonomy of components identified in Figure 2.32 from the review of current serious cyber security games in Section 2.5 Serious Games for Cyber Security and not be restricted to one type of game (research aims and objective 1 & 2).

Part II

Create a New Serious Cyber Game

Chapter 3

Serious Game Design Decisions

This chapter reports the major design decisions of the game designed in Chapter 4. First, the design goals of the game (Section 3.1), an overview of the principles of constructivism learning theory that have driven the game design (Section 3.2), a justification of why a card game is the appropriate learning environment to implement constructivism principles (Section 3.3), why have a games master (Section 3.4), gamified competition or cooperation? (Section 3.5), should be based on real-world or alternative reality? (Section 3.6), should the game content be embedded or not linked (Section 3.7), the selected target audience (Section 3.8) and the conclusions (Section 3.9).

3.1 Design Goals

The primary goal is *to create a learning environment that helps to increase players' awareness of cyber security attacks and the possible countermeasures that can deploy to deter or mitigate them.* The design goals include :

- It conveys the breadth of vulnerabilities and attack methodologies that attackers can exploit.
- It is improving the diversity of possible countermeasures that consider preventing, detecting, or mitigating cyber attacks.
- Players can reflect and understand the possible consequences of risk management decisions within a company.

A serious game that achieves these goals will enable players to become aware and experiment with cyber security concepts applied to real-world scenarios, yet within a calming educational environment.

3.2 Constructivism Principles

The principles of constructivism will be used to design the game learning environment, which has been the predominant learning theory used in education programs for young children, college and university students (Fosnot and Perry, 1996). The constructivism theory is based on the belief that learning occurs as learners are actively involved in meaning and knowledge construction instead of passively receiving information (Rolloff, 2010). In a constructivist learning environment, learners work primarily in groups. Learning and knowledge are interactive and dynamic. There is a great focus and emphasis on social and communication skills and collaboration and exchange of ideas. Contrary to traditional learning environments where learners work primarily alone, learning is achieved through repetition, and the subjects are strictly adhered to and guided by a textbook. In particular, the characteristics of a constructivist learning environment are as follows (Maor, 1999b):

- *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 be active in ways that promote self-direction, creativity, and critical analysis to allow the learning 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 and reflect on their ideas and one of their peers.
- *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 encouraging learners' inquiry by asking thoughtful, open-ended questions and encouraging learners to ask each other questions. Seek elaboration of learners' initial responses; encourage learners to engage in dialogue with the teacher and one another; and provide hints and corrective feedback on their responses/solutions to a problem.

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

3.3 Why a card game?

A tabletop card game can be designed to exhibit all the characteristics of a constructivist learning environment. In particular, the following design principles have been pursued.

- *Simulated Authentic Learning (C1).* One of the critical components of the Riskio game is the game board which represents a real-world scenario with different types of assets to be protected from a cyber attack.
- *Active Learning (C2).* The game adopts role-playing to promote active players' learning: the players impersonate both the role of the attacker and defender on the assets that are part of the scenario. The role-playing 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 cyber security concepts through interaction with the other players and the game master.
- *Interactive Teaching (C4).* It was deemed essential to have a game master at facilitating the construction of players' knowledge. The game master' 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.

3.4 Why have a games master?

One of the games masters' roles is to increase players' intrinsic motivation and achievement. The key to this is using Bloom's taxonomy (Bloom et al., 1956) as a guide in getting the players thinking from lower-order thinking skills of retention through to understanding, applying, evaluating, creating and higher-order thinking skills. The game mechanics and games master role must support this. One method is to ensure the design uses the four elements that have proven to be successful in game design (Stott and Neustaedter, 2013), 1) Freedom to fail, 2) Rapid feedback, 3) Progression and 4) Storytelling, see Table 3.1 for examples of the games master role in Riskio.

Table 3.1: Game Design the Games Master Role.

Games Design	How used in Riskio
Freedom to fail	Players can experiment and encourage to think about attacks and defences
Rapid feedback	Games master gives feedback at the end of each round
Progression	Games master can use Scaffolding by framing, guiding and supporting using the information deck of cards
Storytelling	Games master can give examples through the game board and can be supported by additional case studies can be used to aid the story and new facts revealed through information cards

3.5 Gamified Competition or Cooperation?

Games can be designed using gamified competition or gamified cooperation. Both can facilitate similar learning and motivational outcomes (Dindar et al., 2021; Morschheuser et al., 2019). Examples of gamified competition are game scoring or levels players go through the game and examples of cooperation one where players can collaborate to find solutions to problems. The game will be designed for both gamified competition and cooperation.

3.6 Real-World and Alternative Reality

McGonigal (2011) proposes Alternative Reality Games (ARGs) to bring gameplay into day-to-day experiences. ARG games feel like real life but capture the four essentials of gaming: goals, rules, feedback and voluntary participation. ARGs is played in a real-world context and designed to make it easier to generate four intrinsic rewards: more satisfying work, better hope success, more robust social connections and more meaning (McGonigal, 2011). Any serious game needs to include a high level of realism to ensure user training and education (Chalmers and Debattista, 2009). We decided to create the game based on a fictional organisation of the University Fees Office.

3.7 Endogenous or Exogenous Design?

Designing serious games could be done by two approaches, endogenous or exogenous (Mestadi et al., 2018; Mancuso et al., 2013). The endogenous or intrinsic approach proposes that the domain content and game should be naturally embedded or linked. For example, in cyber security, embed published government standards on defence in the gameplay. The alternative exogenous approach or extrinsic approach considers that the domain content and the serious game are unrelated. In serious exogenous games, the player could win points by gaining access to information or questions unrelated to the gameplay. However, we decided to take an endogenous approach for serious cyber games and link the domain content in the gameplay.

3.8 Target Audience

The target groups for the game will be a critical factor in the design and development of the game. If more than one target group for the serious game, this may require adaptation mechanisms for different learning styles (Rapeepisarn et al., 2008). Targeting one group could leave other groups disengaged and not meet the game's objectives. The suggestion is that games developers should consider segmentation based on the two main categories of gamers: hardcore and casual (Ip and Jacobs, 2005). The primary audience is executives, senior managers and operational staff

(possible casual gamers) who can understand business risks from adopting new technology or the new regulations. Still, they lack technical knowledge about risks coming from cyber threats. The secondary audience was identified as students (possible hardcore gamers) with specialised expertise in IT infrastructures, but they lack knowledge on applying for protection from cyber attacks in business contexts. To measure the gaming behaviour, further segmentation was considered: Demographic, Psychographic and Behavioural (Tuunanen and Hamari, 2012) to verify the players' typologies, see Table 3.2.

Table 3.2: Example of Segmentation of Players.

Segmentation	Target Groups	Game Design
Demographic	*Students*: Limited work experience. *Employees:* Range of work experience	Game board designed suitable for both groups
Psychographic	*Students:* Hardcore game players. *Employees:* Casual gaming experience	Additional game mechanics can be added for students
Behavioural	*Students:* Single oriented player. *Employees:* Social mentalities	Option for more experienced students to play for points

3.9 Conclusion Design Decisions

In this chapter, we identified the initial design decisions used to create the game in the next Chapter 4 to design a new serious game to identify the critical elements of pedagogical models to design serious cyber games. The design decisions may change as we learn from creating the serious game. See Table 3.3 for a summary and additional thoughts of crucial design decisions.

None of the serious games reviewed in the literature review (see games reviewed Section 2.5) met the research aims and objectives in Section 1.3. We decided that the Elevation of Privilege (EoP) game had the most scope to be changed to meet these objectives (see 2.5.1 for EoP Game), although it was noted that EoP was designed for secure software development. The EoP game has the most significant capacity to adapt to testing and learn the game mechanics to create a pedagogical model. Key benefits of using EoP:

- The game board can easily be created and changed using Microsoft Visio.
- The EoP game cards can be downloaded under a creative comms licence and can be edited and changed as required (Creative Commons, 2018).
- The game uses a well-known threat model Microsoft STRIDE.
- It will be easier to test different gameplay using a tabletop card game than a computer-based game which might require re-coding.

Table 3.3: Initial Serious Game Design Decisions.

Design Elements	Comments
Design Goals	To meet the research objective, must provide a breadth of vulnerabilities and attack methodologies that attackers can exploit.
Constructivism Principles	Constructivism is a learning theory that explains how people might acquire knowledge and learn. (Bada and Olusegun, 2015)
Why a card game?	Cards can easily and quickly be changed and will help in developing the gameplay quickly.
Why have a games master?	The games master will be able to get feedback from players.
Gamified Competition or Cooperation?	Design a game so we can test both options.
Real-World and Alternative Reality	The fictional organisation will give more opportunities for players to identify threats and countermeasures.
Endogenous or Exogenous Design?	We want to build the domain content into the game as key to the serious game objective.
Target Audience	Using both students and employees gives a wide range of backgrounds for players.

The Microsoft EoP game will be used as a base of the design in Chapter 4 of Riskio, a new security game.

Chapter 4

Riskio a New Security Game

This chapter is about how Riskio was developed and designed, the game objectives, the required experience of the games master and game players, the rationale for designing the cards and game boards, and how the game is played. Section 4.1 is the background of the development of the Riskio game. Section 4.2 is about the Riskio game objectives. Section 4.3 is about the game tutorial before the players play the game. Section 4.4 explains the game components, cards and game boards. Section 4.5 explains the game mechanics and gameplay using an example of attack and defence. Section 4.6 is the initial conclusion on the Riskio game before verification in testing with target players.

4.1 Game Development

The base game development (see subsection 4.1.1) was based on the Microsoft EoP Game (see subsection 2.5.1) and used Microsoft rules and STRIDE threat methodology, see Table 4.1. This was played between research team supervisors and academic staff at the University of Southampton. See Figure 4.1 for an example of the first deck of cards. After changes were made from feedback, the cards were printed professionally, ready for the next stage, where Riskio was played to test the desired hypothesis questions in the formal experiments. Changes were made to the cards between the formal experiments from players feedback, and the game was updated cards re-printed and played again (see subsection 4.1.2).

Table 4.1: Microsoft STRIDE Threat Model Taxonomy.

Threat	Property we want	Example of Threats against
Spoofing	Authentication	Attacks to procedures can 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	Integrity	Attacks that alter data at rest, e.g. by exploiting a vulnerability in application front-ends or transit, e.g. due to a lack of message encryption
Repudiation	Non-repudiation	Threats to claim to have not performed an action. The cards allow the creation of attacks against logging functionality, the auditing process and insufficient user authentication
Information Disclosure	Confidentiality	Threats to the confidentiality of information. The cards allow the creation of attacks exploiting inadequate encryption procedures for data at rest and in transit, flawed system configurations and non-adequate user security policies
Denial of Service	Availability	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	Authorisation	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

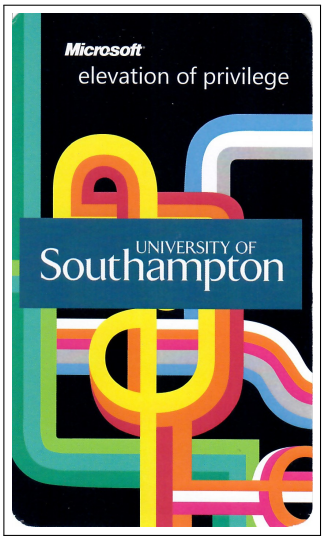
4.1.1 Base game development

The first game, referred to as the 'Base Game', was based on the Microsoft Elevation of Privilege game (Microsoft, 2018) which is freely available to download and amend under a Creative Comms license (Creative Commons, 2018) (see Section 3.9).

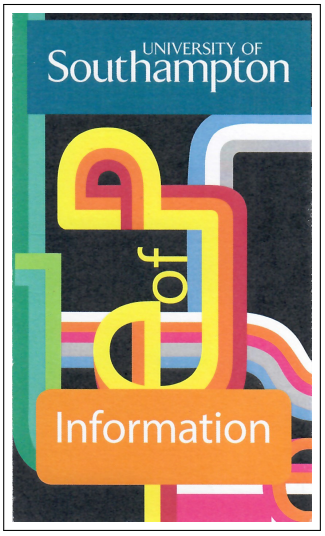
Figure 4.1: Home Printed Cards - Base Game Development (Cards V1).

Version 1: Base Game EoP. The game was printed using a home printer to test the game, and the only change was to the questions on the cards. The gameplay used Microsoft rules and is based on Microsoft STRIDE threat methodology, see Table 4.1.

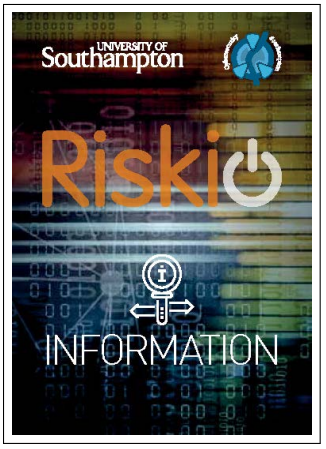
Feedback The game is only based on attacking; The game was based on data flow diagrams, see Figure 4.11; and Questions were very technical. **Changes for V2:** Add defence stage; Add network diagram, see Figure 4.10; Update questions to be less technical; Create notes on possible attacks and defences for the Games Master for all six attack suits, see Appendix G for Spoofing suit example. The game was then updated and sent for professional printing to create version 2 (v2) of the cards (see Subfigure 4.2(a)) ready for the start of formal testing.



(a) **Card V2** used Experiment 1 (Size 70 x 120 mm)



(b) **Card V3** used Experiment 2 (Size 70 x 120 mm)



(c) **Card V4** used Experiment 3 & 4 (Size 64 x 90 mm)

Figure 4.2: Riskio Card Versions for Formal Experiments 1 - 4 Changes from Player Feedback.

4.1.2 Formal experiments to test and develop game

The start of the formal experiments. This point was the beginning of the four experiments, see Appendix N for ERGO Application and Appendix O for Data Protection Plan. All participants were given a participant information sheet, see Appendix C, and this explained the background to the research, how their data will be processed to ensure informed consent. The participants who agreed to take part were required to complete a consent form, see Appendix D.

Experiment 1: October 2018 at the premises of a company member of the CSA.

- **Version 2: Base Game EoP v2** (V2 cards used, see Subfigure 4.2(a))

  Players Comments (pc): 1. Cards too large to hold; 2. Players did not want to play the game rule option of cards face up; 3. Players spent a long time selecting attack cards; 4. The player did not understand the EoP Trump card rule; 5. Players confused by theme colours; 6. Players were confused by the design, why Jack, Queen and King?; 7. Proposal to play one person as an attacker and others as defenders.

  Changes for V3: Change to add STRIDE suit to back of the card and players select one card at a time (pc2, pc3); Remove Trump card rule (pc4); Change theme colour to Red Attack; Green Defence; and Yellow Information (pc5); Change design of Jack, Queen & King (pc6); Change game rules (pc7); Add new game board, office diagram, see Figure 4.9 and University Fees Case Study, see Appendix A, gives a background to office diagram for the players.

Experiment 2: October 2018 during the Secure Software Development course taught at the University of Southampton.

- **Version 3: Base Game EoP v3** (V3 cards used, see Subfigure 4.2(b) and gameplay Figure 4.3)

  Players Comments: 1. Cards too large (70mm x 120mm); 2. Lack of images on the cards; 3. games master found it difficult to award 1 point; 4. Change to the game from two stages from attack and then defence.

  Changes for V4: Change card size to 64mm x 90mm (pc1), see Subfigure 4.2(c); Add images to the cards (pc2); Change rules to allow for up to 3 points (pc3); Players take turns to act as attacker and other players defend (pc4).

  Add new Riskio Logo and Images; Further changes and updates to card wording and design, see Figure 4.4.

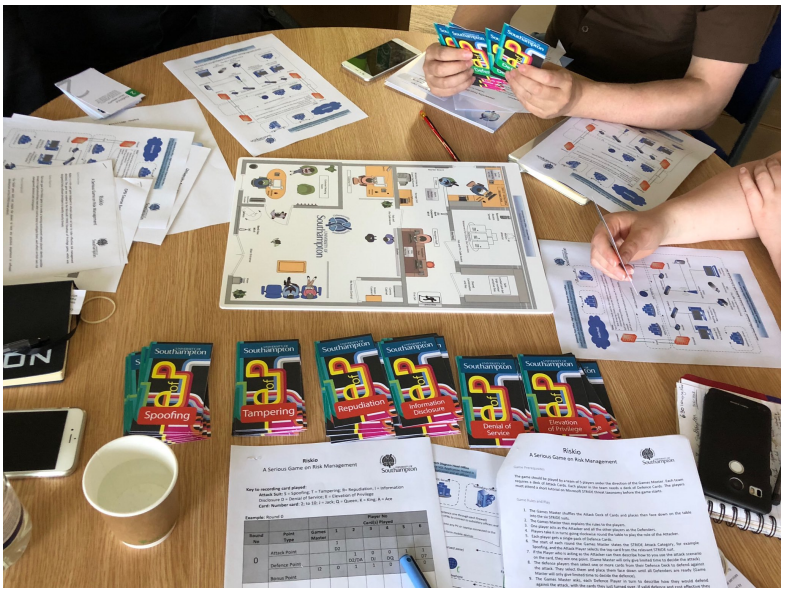


Figure 4.3: Experiment 2 - Gameplay Card Version 3 (V3).

Experiments 3 & 4: 3: January 2019 as part of a professional training course on "Cyber security awareness" & 4: April 2019 as part of a professional training course for "Chief Data Officers".

- **Version 4: Riskio Created** (V4 (Riskio) cards used, see Subfigure 4.2(c))
- No further changes made to cards

4.2 Game Objectives

Riskio is a security card game designed to educate players on how to make effective risk management decisions. The game was inspired by the Microsoft STRIDE Elevation of Privilege game (Wuyts et al., 2014; Williams and Yuan, 2015), designed to help software developers identify security threats.

The main goal of the Riskio game is to create a learning environment where players identify possible threats to organisational data, learn what could be done to mitigate them and reflect on their own risk management decisions and consequences.

The Riskio game objectives are:

- Create a fun and engaging learning environment
- Increase cyber security knowledge of the players
- Cover a wide range of vulnerabilities and mitigations
- Understand costs, limitations and implications of controls
- Adaptable to different organisations and players' background

(a) Riskio 2 of Spoofing

(b) Riskio 2 of Information

(c) Riskio 2 of Defence

Figure 4.4: Example of Riskio Game Decks Final Design Versions.

4.3 Game Tutorial

Before playing the game, all the players were given a brief tutorial on the Riskio game, including a briefing on the Microsoft STRIDE threat model and NIST five functions (NIST, 2021b). The presentation on STRIDE was to help them to think about a broader range of attacks (Figure 4.5).

The NIST five functions (NIST, 2021b) see Figure 4.6, were included in the pre-game tutorial to teach players that there may be more than just a "Protect" defence strategy. Threat actors that are highly sophisticated and skilled, for example, state threat actors, require alternative defence strategies, such as 'Detect' and 'Recover' from some attacks. The tutorial also gave examples of different strategies for defence (see Figure 4.7) and, if scoring is used, the game scoring (see subsection 4.5.3).

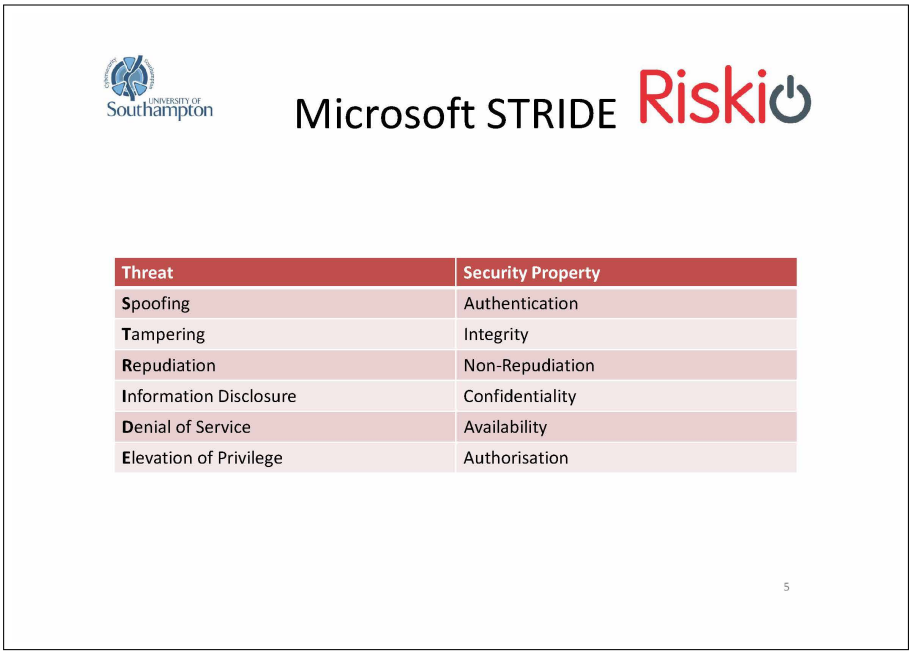


Figure 4.5: Riskio Game Tutorial Slide 05 - Microsoft STRIDE Threat Model.

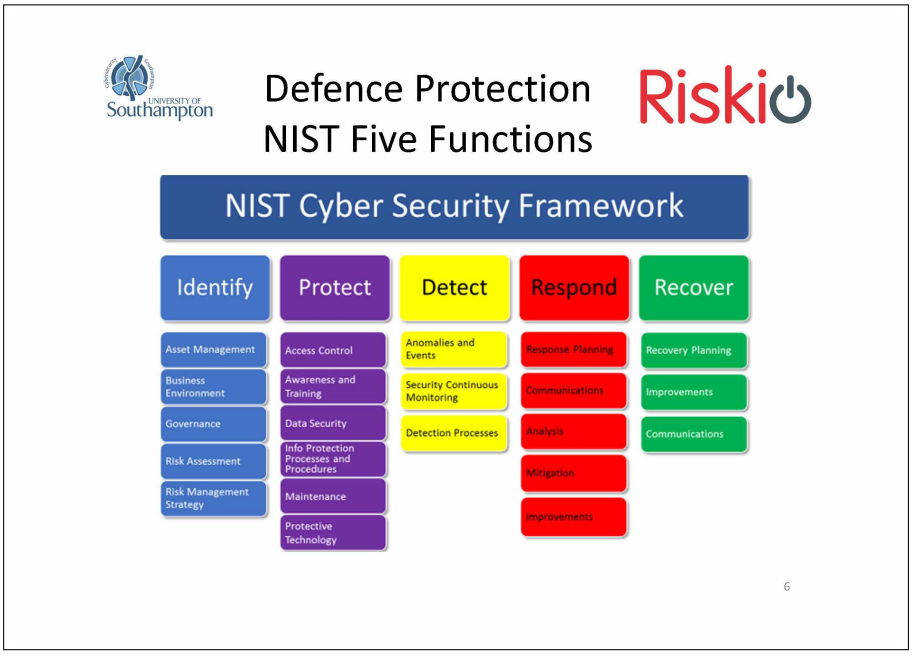


Figure 4.6: Riskio Game Tutorial Slide 06 - NIST Cybersecurity Framework's Five Functions.

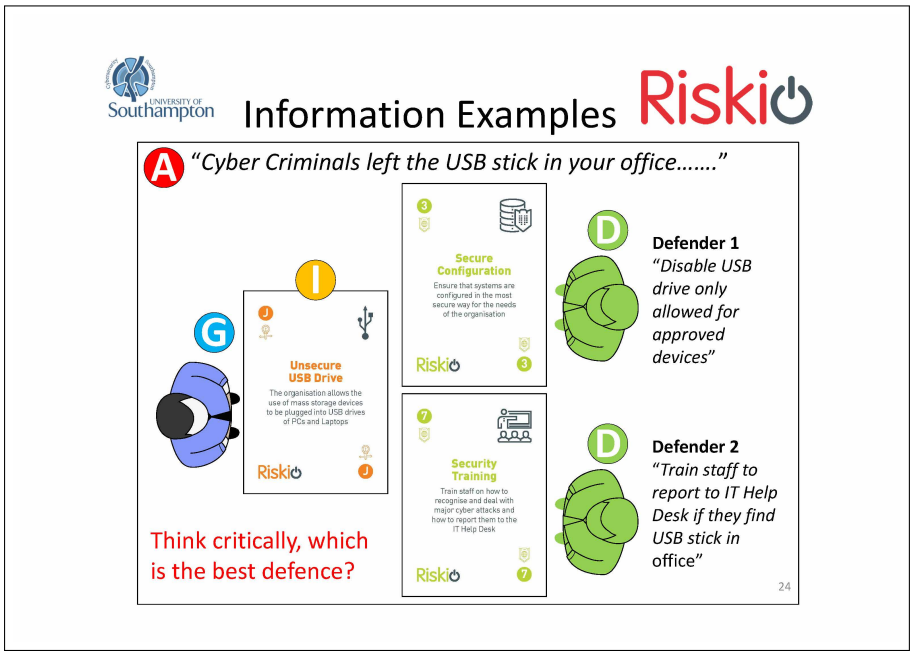


Figure 4.7: Riskio Game Tutorial Slide 24 - Example of Defence in Riskio Game.

4.4 Game Components

The key components of the game are the **Games Master**, ***Card Decks*** and the ***Game Boards***.

4.4.1 Games Master

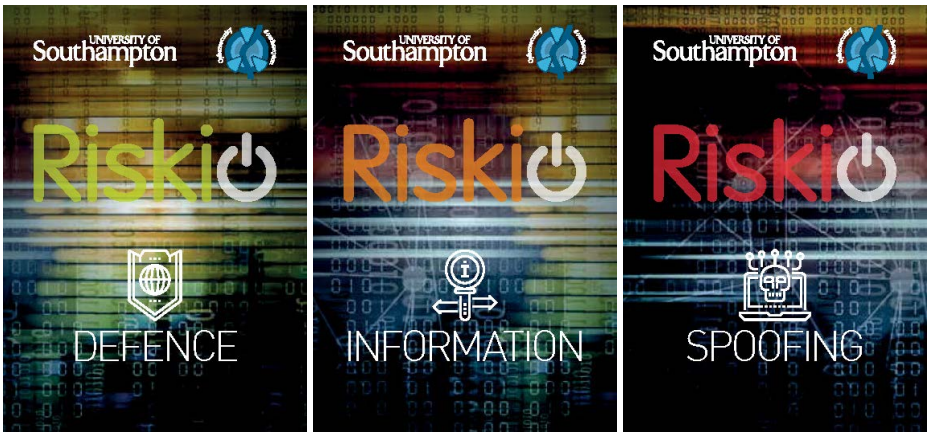
The Riskio games master needs to be an experienced cyber security professional and experienced teacher with experience in the following standards:

- Microsoft STRIDE threat model
- OWASP Top 10 Most Critical Web Application Security Risks
- ISO/IEC 27001 information security standard 114 controls objectives (ISO/IEC, 2021)
- NIST SP800-39 Risk Management Information security standard (NIST, 2011)
- Degree in related subject area Computer Science / Cyber Security
- Current Cyber threat trends
- Mitigations to cyber vulnerabilities
- NCSC Cyber Essentials (NCSE, 2020)
- NCSC 10 Steps to Cyber Security (NCSC, 2021)

4.4.2 The Card Decks

The Riskio game has three decks of cards: Attack Deck, Defence Deck and the Information Deck. See Figure 4.8 for an example of Riskio three card decks. The design colour was based on: Attack

Deck was Red, for warning of attack; Information Deck was Amber, which could be helpful information to help with defences; and Defence Deck was Green, for good defences, making each of the decks identifiable. See Appendix B for a complete list of all the Riskio card decks.



(a) Defence (b) Information Deck (c) Attack Deck (6 STRIDE Suits)

Figure 4.8: Riskio Game Card Decks Back of Cards.

4.4.2.1 Attack Deck

The attack deck is formed by six suits of 13 cards (the same as a typical card deck: Ace, 2 to 10, then Jack, Queen and King). Each suit of the attack deck was based on categorising the attacks based on the six Microsoft STRIDE threat categories. See Table 4.1 for an example of an attack for each of the STRIDE threat categories.

4.4.2.2 Information Deck

The information deck is formed by a single suit of 13 cards: 2 to 10, then Jack, Queen, King and Ace, see Figure B.8 representing security-related events resulting in a successful cyber attack unless the correct defence card is played. The games master uses this deck to test players' defence strategies and help the gameplay. The games master can also play the Ace card and add their own information. This deck was added after feedback from NCSC, and they suggested adding shock value. For example, in the previous round, the games master says, "you were told about a vulnerability of a web application only having a username and password to access it. You have now been told the web application has 10,000 users. Does this change your defence strategy and why?". This example is to test players to understand how this increases the risk from the attack.

4.4.2.3 Defence Deck

The defence deck is formed by a single suit of 13 cards: 2 to 10, then Jack, Queen, King and Ace, see Figure B.7 representing the core security controls that can be directly applied to mitigate against known attack types. The cards are based on NCSC Cyber Essentials. However, there are limitations to Cyber Essentials, that it was designed for SMEs, does not consider cloud services and does not consider the information asset values. The 10 Steps to Cyber Security (NCSC, 2021) was added as possible defences to overcome this issue. The Ace defence card allows more experienced players the opportunity to reference more detailed defence controls, for example, Center Internet Security (CIS) Top 18 Critical Controls see Table 4.2.

Table 4.2: Riskio Game Defence Controls.

Assurance Standards	Controls
NCSC, Cyber Essentials Scheme (Continuity and Forum, 2018)	Cyber Essentials is a UK scheme of recommended five basic technical controls to help protect organisations against common online security threats
NCSC 10 Steps to Cyber Security (NCSC, 2021)	The ten steps to creating an effective organisational risk management regime, from risk management, technical controls to awareness and education
The 18 CIS Controls (v8) (CIS, 2021)	18 controls group by task-based, which contain 153 safeguards (security controls). Safeguards prioritised implementation groups (IGs), IG1 Basic Cyber Hygiene, IG2 and IG3

4.4.3 Game Boards

The Riskio game can be played with three Game Boards. Each game board can be adapted to represent the organisation that the game players must consider the possible threats and defences to protect the organisation data and services. The Riskio game board can be tailored to a scenario that the players are familiar with their organisation.

The game boards have different strengths and weaknesses: Office Diagram (see subsubsection 4.4.3.1 and Figure 4.9), Network Diagram (see subsubsection 4.4.3.2 and Figure 4.10) and Data Flow Diagrams (see subsubsection 4.4.3.3 and Figure 4.11). The game can be played with one or more of these types of game boards.

4.4.3.1 Game Board: Office Diagram

- Suitable for physical security vulnerabilities
- Needs little explanation
- Requires more thought to find possible technical vulnerabilities
- Found in games testing to be liked by both technical and non-technical players

Comments: Supported with case study explaining office processes. Most understood by senior managers and could use actual office plans.

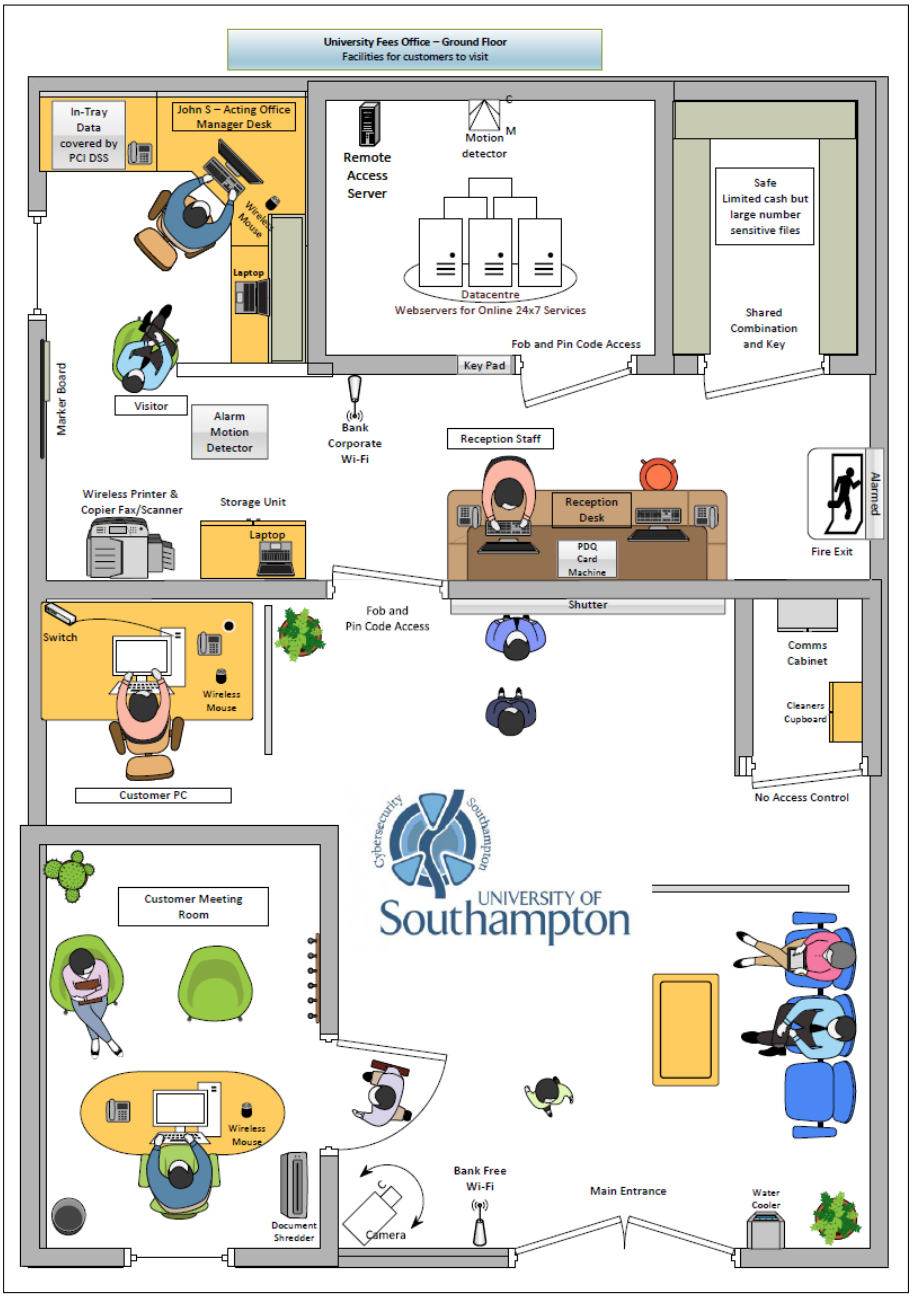


Figure 4.9: Riskio Game Board: Office Diagram.

4.4.3.2 Game Board: Network Diagram

- Good for technical vulnerabilities
- The network diagram could be used as a side-b to office diagram game board (see Figure 4.9)

Comments: For some players need to explain network components and what they do.

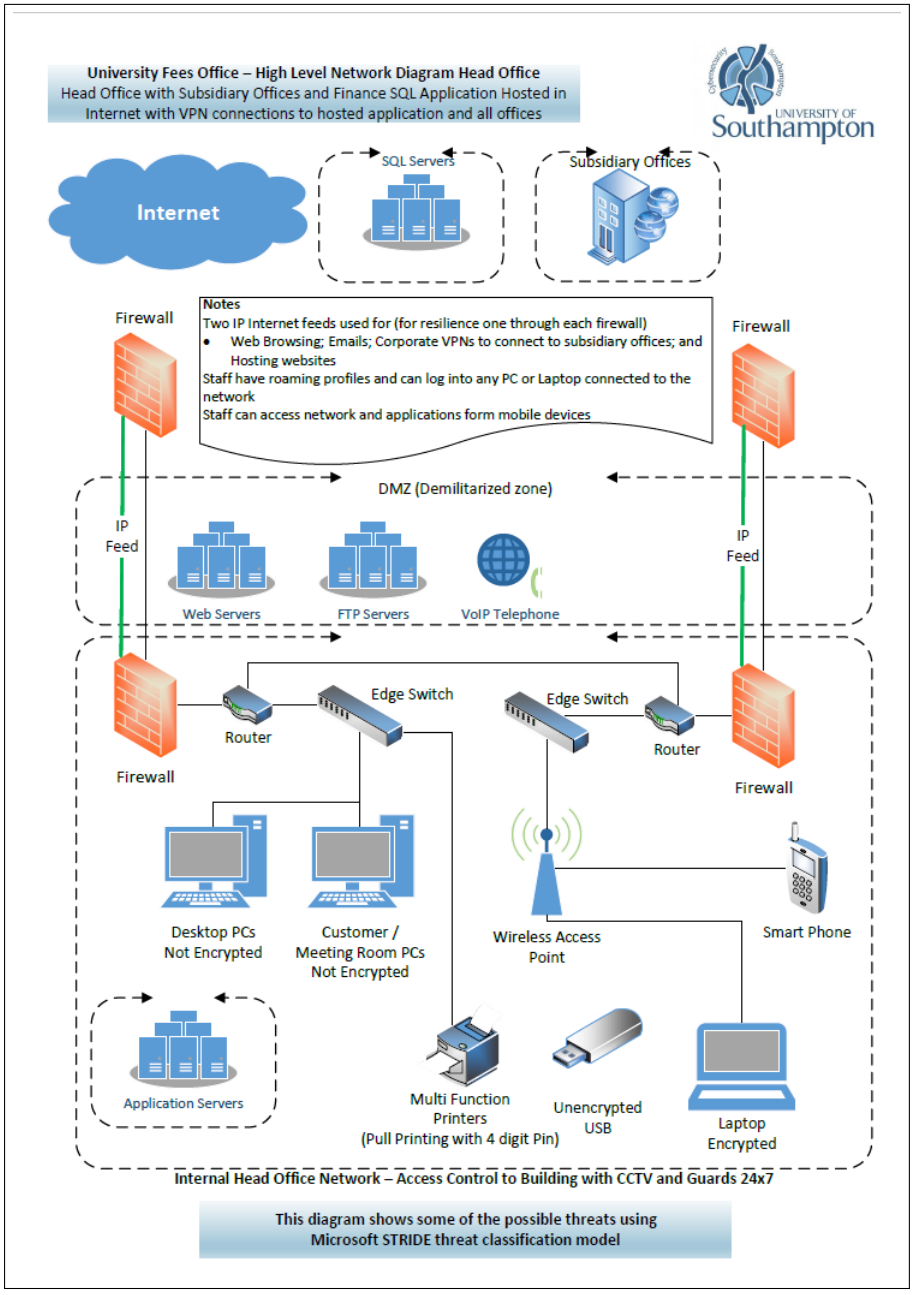


Figure 4.10: Riskio Game Board: Network Diagram.

4.4.3.3 Game Board: Data Flow Diagram

- Best for critical services to identify low-level technical vulnerabilities
- Practical as Microsoft EoP Game subsection 2.5.1 to conduct threat modelling as part of the design phase of software projects

Comments: We needed to explain the diagram to the players unless players created a diagram as per the EoP game subsection 2.5.1.

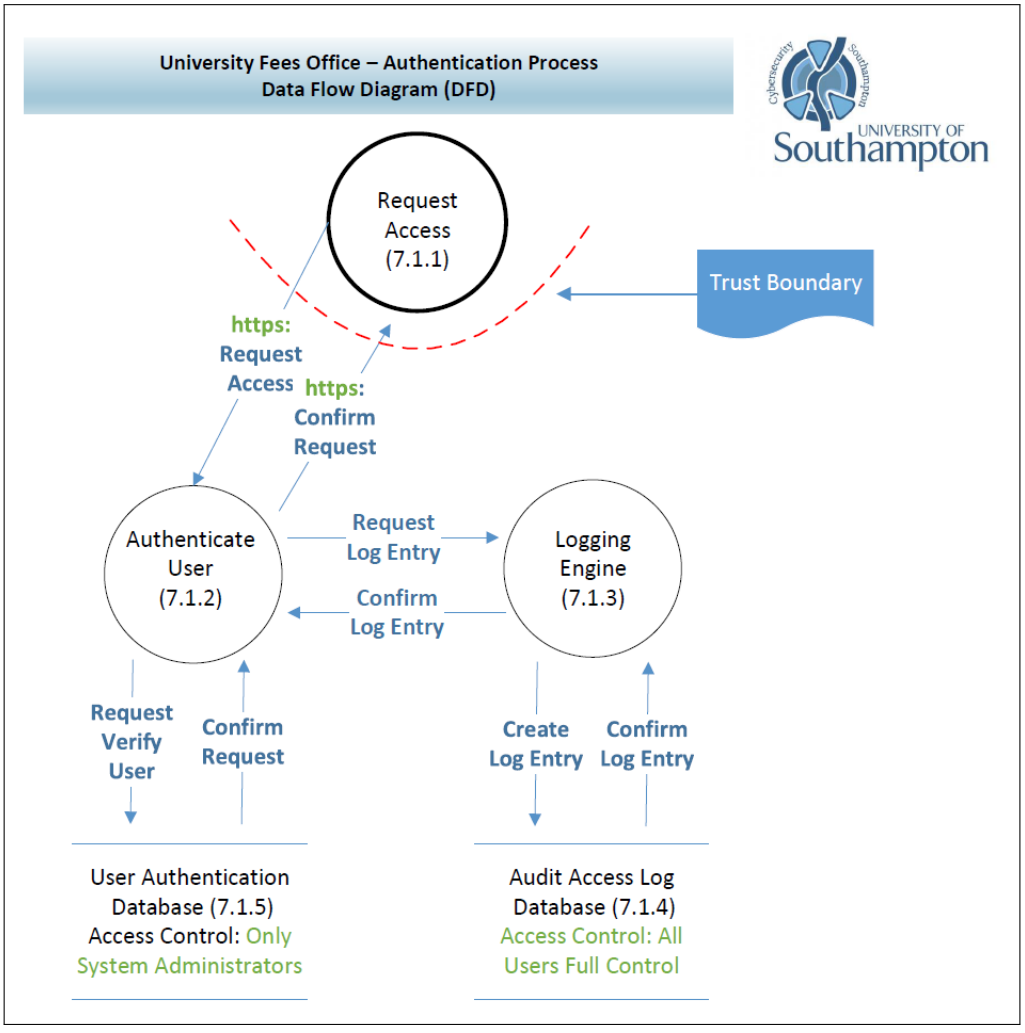


Figure 4.11: Riskio Game Board: Data Flow Diagram.

4.5 Game Mechanics and Play

The Riskio game should be played by a team of between 3 to 5 players under the direction of the games master. Each team requires a deck of Attack Cards. Each player in the team needs a deck of Defence Cards. The players must attend a short 30-minute tutorial on Microsoft STRIDE threat taxonomy before the game starts (see Section 4.3).

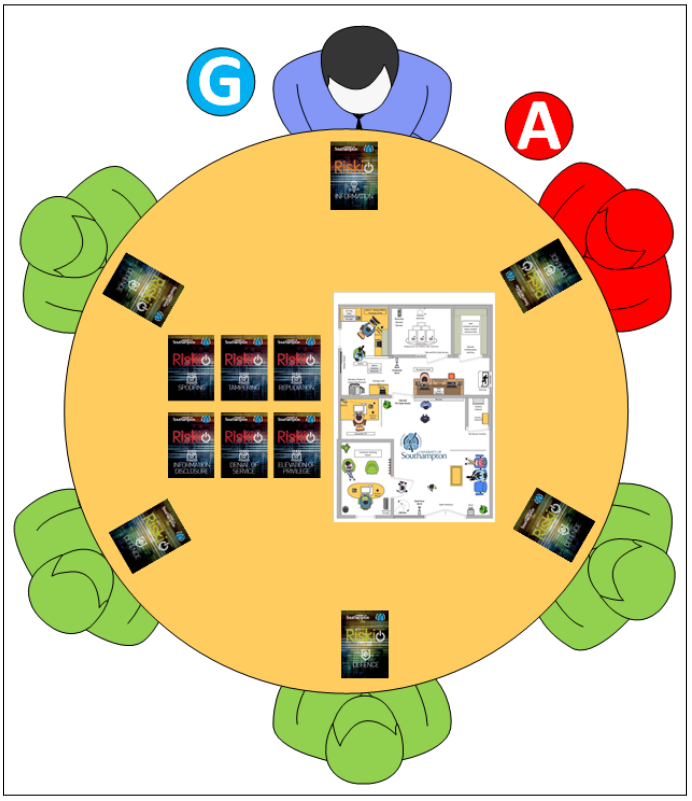


Figure 4.12: Riskio Game Setup - Games Master (G) Attacker (A).

The game mechanics are structured into both attack and defence phases. Typical gameplay would request players to sit around a table with the game board in the centre (see Figure 4.12). 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:

4.5.1 Attack Phase

The game starts with the first player to the left of the game master acting as the attacker, and all the other players as the Defenders (see Figure 4.13). The attacking player selects the top card from a chosen attack suit, 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 incorrect, the game master will provide an example of an attack explaining who and how the attack could be conducted.

Figure 4.13: Riskio Game Attack Stage - Games Master (G) Attacker (A) Defenders (D).

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 cybercriminal gathers information from a university website and uses this to create emails to target John, the Office Manager". 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."*

4.5.2 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 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 spot spoofed emails and implement an intranet-based training solution for staff to test their skills". Defender 2 instead selects the "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 no". 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 a process to report phishing emails should be used in combination to defend against spear-phishing attacks effectively. The defence proposed by Defender 2 - blocking phishing emails - may not be effective because often attackers spoof legitimate email addresses".

4.5.3 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 concerning confidentiality, integrity and availability for the organisation (see Figure 4.14). 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 (see Figure 4.15). It was noted that the majority of players preferred the feedback from the games master over the scoring and working in cooperation in defending over the gamified competition.

4.5.4 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, see Figure 4.16.

Example 4.3. *Games master selects the "Jack of Information - Unsecured USB Drive" and states, " A cybercriminal left a USB stick in the office, and a staff member has plugged it into his office computer. Since the USB key was infected by 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 usernames and passwords". All players now play the role of the Defender and select defence cards 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 software". Defender 2,*

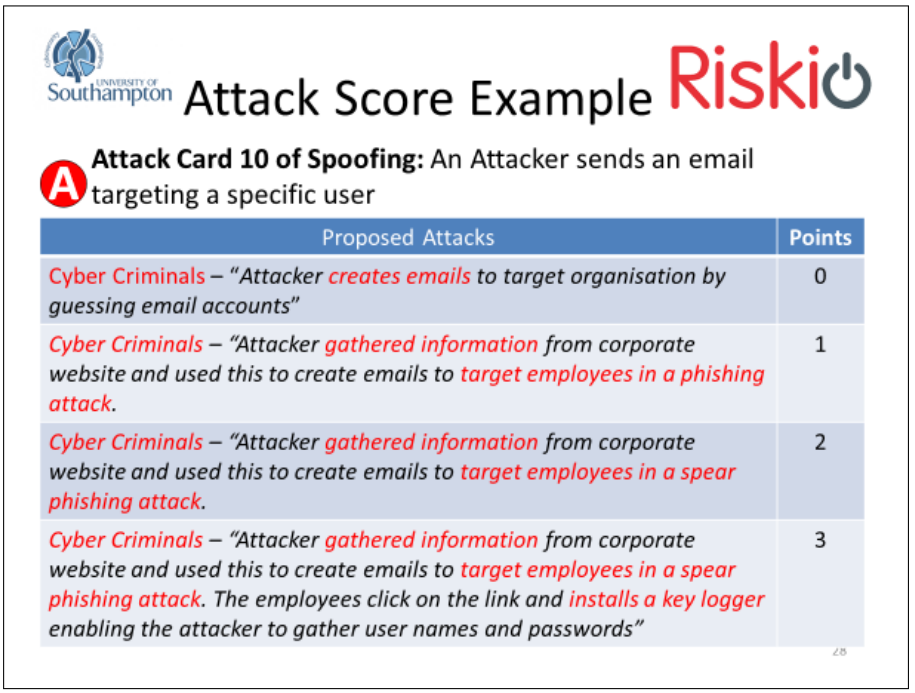


Figure 4.14: Riskio Game Tutorial - Attack Example 10 Spoofing.

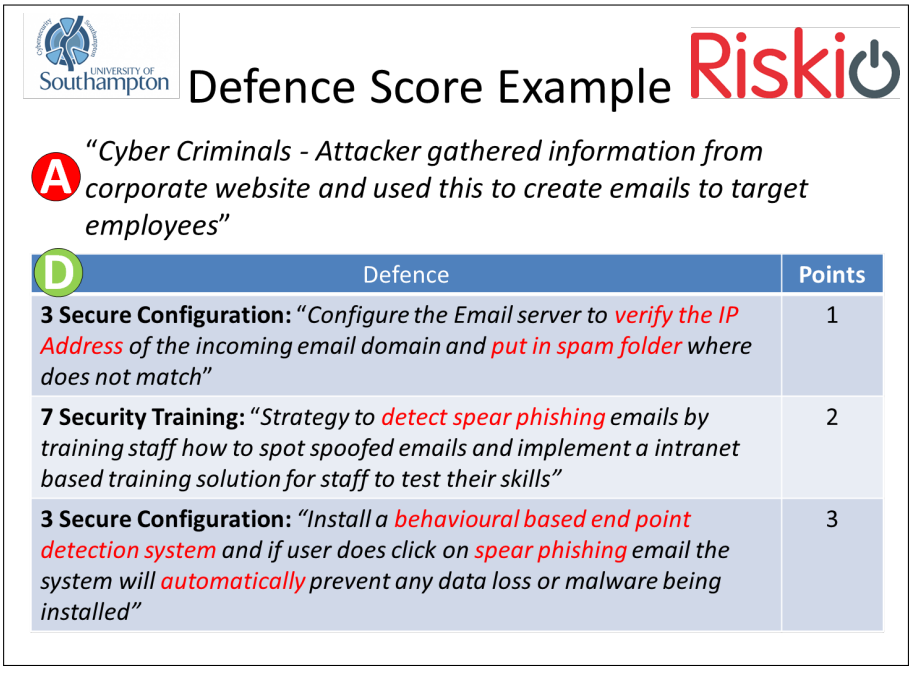
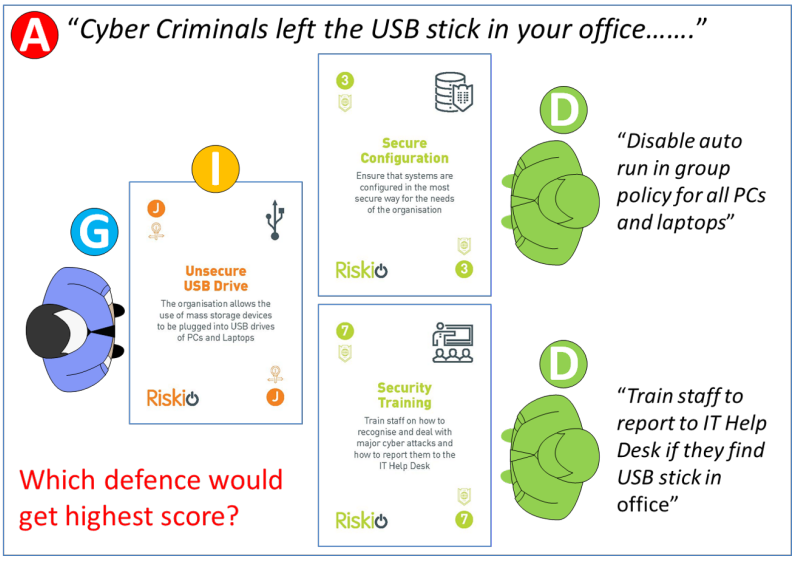


Figure 4.15: Riskio Game Tutorial - Defence Example.

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 the 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".



Information Phase Example of Games Master acting as the attacker

Figure 4.16: Riskio Game Tutorial - Riskio Game Setup.

4.6 Conclusion Riskio Design

From the gaps identified in Section 2.12, the literature review in Chapter 2 of serious cyber games Riskio game design has improved on these by:

Improvement 1: The Riskio game boards and cards can be changed to create different game scenarios to meet different learning objectives based on organisational requirements (Issue 2 and Issue 5).

Improvement 2: In the Riskio gameplay, the players can act as the attacker and the defender (Issue 3).

Improvement 3: The Riskio questions can be designed to balance between technical and non-technical players or could be designed for either group (Issue 4).

Improvement 4: The Riskio game can be played using gamified competition, by using the scoring option or gamified cooperation, change rule players defend together (Dindar et al., 2021; Morschheuser et al., 2019).

In the next Chapter 5, the Riskio game will be formally evaluated. However, although Riskio has made improvements over games reviewed in the literature review, it should still be noted. It still does not close the gap on the primary requirement in the research aims and objectives (see Section 1.3) as it does not provide a design model to create other serious cyber games (research aims and objective 1).

Chapter 5

Riskio Game Evaluation and Conclusion

This chapter presents the study design (Section 5.1), study realisation (Section 5.2), analysis of the study results (Section 5.3), threats to validity of the case study (Section 5.4), discussion and reflections (Section 5.5) and the conclusion (Section 5.6).

5.1 Riskio Study Design

Before conducting the study, Riskio has been evaluated through several rounds during the design and the development phase. The ease of understanding the attack and defences on the cards and the game's mechanics were tested. To conduct the playtest and the study, we obtained ethical approval from the University of Southampton's Ethics and Research Governance Online (ERGO) system (Submission ID: 44919, see Appendix N). Playtests were conducted with security experts, doctoral and postdoctoral students in computer science, and employees in organisations. Feedback provided in this phase has been incorporated in the final version of the game evaluated during the study. The opinions of the players on the usage of the games be captured through using observation and asking questions (Hursen and Bas, 2019).

Robson and McCartan (2016) propose when conducting a case study it is a significant strength to use multiple sources of evidence (Lorås, 2017). The method used was to use both the post-game questionnaire and observation to avoid any bias in just a single source of evidence from the questionnaire. Robson and McCartan (2016) also proposes an increased emphasis on ethical issues, in line with greater awareness of the rights of research respondents (Goodenough and Waite, 2012). All the playtests respondents had to opt-in to take part in the study and signed a consent form (see Appendix D).

5.1.1 Riskio Questionnaire

The design of the study was based on the Technology Acceptance Model (TAM) (Davis, 1989; Yusoff et al., 2010), 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), person's subjective probability that using a particular system would enhance their job performance; 3) Intention to Use (ITU), the extent to which a person intends to use a particular system.

Two questionnaires were created to statistically evaluate the Riskio gameplay and player views on security games.

- **Questionnaire 1 - Participants Background and Security Awareness**, see Appendix E - To verify the players' background qualifications, experience and knowledge in cyber security
- **Questionnaire 2 - Riskio Game Assessment**, see Appendix F - Evaluate the players' impressions on playing the Riskio game (not to evaluate how well they played) and a section on views of security games

Questionnaire 1 and questionnaire 2 asked the players questions on a Likert scale of 1 to 5. Because both the groups that played had low numbers, the methodology used to evaluate was Boxplot Diagram and showed the outliers plotted as individual points. The calculation for the outliers was based on Interquartile Range (IQR) to set the minimum and maximum values to be considered, see Equation 5.1.

$$\begin{gathered} IQR = Q_3 - Q_1 \\ Q_1 - 1.5 \quad IQR \qquad Q_3 + 1.5 \quad IQR \end{gathered} \tag{5.1}$$

The study's overall goal 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 easy to understand.
- PU: The players find the Riskio game valuable in increasing awareness of cyber security concepts, focusing 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 the primary and secondary audiences (respectively, employees and students) to identify differences in perception. To this end, a series of experiments were organised involving students and employees who have limited or no knowledge in cyber security and had not previously played the game.

During each experiment, the participants were first provided with a short introduction to the Microsoft STRIDE threat taxonomy, the University fee office scenario and the play rules of the game. Then, they were divided into groups of a maximum of five players and let each group play the game for about 45 minutes under the guidance of a game master. A demographic questionnaire and a post-task questionnaire collected participants' perceptions of the game based on the TAM constructs at the end of the game. This latter questionnaire is reported in Table 5.1 and consists of 16 questions with answers on a 5-point Likert scale. Used the 5-point scale to test the position of neutrality (neutral/do not know = Score 3) lies precisely in between two extremes of strongly disagree (score 1) to agree strongly (score 5) (Joshi et al., 2015). To explain a possible difference in participants' perception, we asked the participants to provide feedback on the game at the end of each experiment.

5.1.2 Riskio Observation

Players were encouraged to give feedback to the games masters in the gameplay on any points that might improve the game. They were asked to provide feedback on anything they did not like or considered could be improved. The players were told in the game tutorial at the start that the game was in development and encouraged to give anonymous feedback (see subsection 5.3.3 for players feedback). The games master could observe and ask players questions. The games masters generally agreed that players were very active in providing constructive feedback on improving the game, what they liked and what they did not like (see subsection 5.3.3). We tried in the first experiment (see Figure 5.10, Game Scoring Sheet) to get the games master to record the attack card and the defence cards that were played. This was abandoned as games master found it impossible to give feedback to players and record cards played without disrupting the game flow.

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 (CSA), a partnership between the University of Southampton and the industry. This experiment involved 14 graduate students newly hired by the company. The background of the participants was heterogeneous: they had BSc in Computer Science, Electrical Engineering, Mathematics, Physics and Game Development. The participants were divided into three groups. The experiment was a constituent part of the induction training on cyber security for all new employees. Two post-task questionnaires were incomplete or not returned.

The second experiment was performed in October 2018 during the Secure Software Development course taught at the 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. Two post-task questionnaires were incomplete or not returned.

Table 5.1: Riskio Game Evaluation Post-task Questionnaire.

No	Type	Question
Q1	PU	I found playing the Riskio Game improved my knowledge of Cyber Security
Q2	PEOU	I found the Riskio Game easy to learn
Q3	PU	Overall, I think playing the Riskio Game provides an effective solution to the identification of cyber threats
Q4	ITU	If the game was adapted based on my organisation, I would use the Riskio Game to identify cyber threats
Q5	PU	Playing the Riskio Game helped me find new threats that I could have not found without playing the game
Q6	PU	Overall, I think playing the Riskio Game provides an effective solution to the identification of cyber defences
Q7	ITU	If the game was adapted based on my organisation, I would use the Riskio Game to identify cyber defences
Q8	PU	Playing the Riskio Game helped me find new defences that I could have not found without playing the game
Q9	ITU	If I need to increase Cyber Security awareness in a future project at work, I would use the Riskio Game
Q10	PU	Overall, I found playing Riskio Game to be useful
Q11	PU	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	PU	Playing Riskio Game made me more productive in identification of cyber threats
Q13	PU	Playing Riskio Game made me more productive in identification of cyber defences (counter measures)
Q14	PU	I feel playing a security card game is a effective method to teach cyber security
Q15	ITU	I feel playing a security card game is a effective method to identify cyber security threats in my organisation
Q16	ITU	I feel playing a security card game is a effective method to identify cyber security defences in my organisation

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 divided into three groups. The participants had different roles within the organisation: C-level, IT Team, Finance Team, Risk/Assurance Team, and practitioner area directors. Two post-task questionnaires were incomplete or not returned.

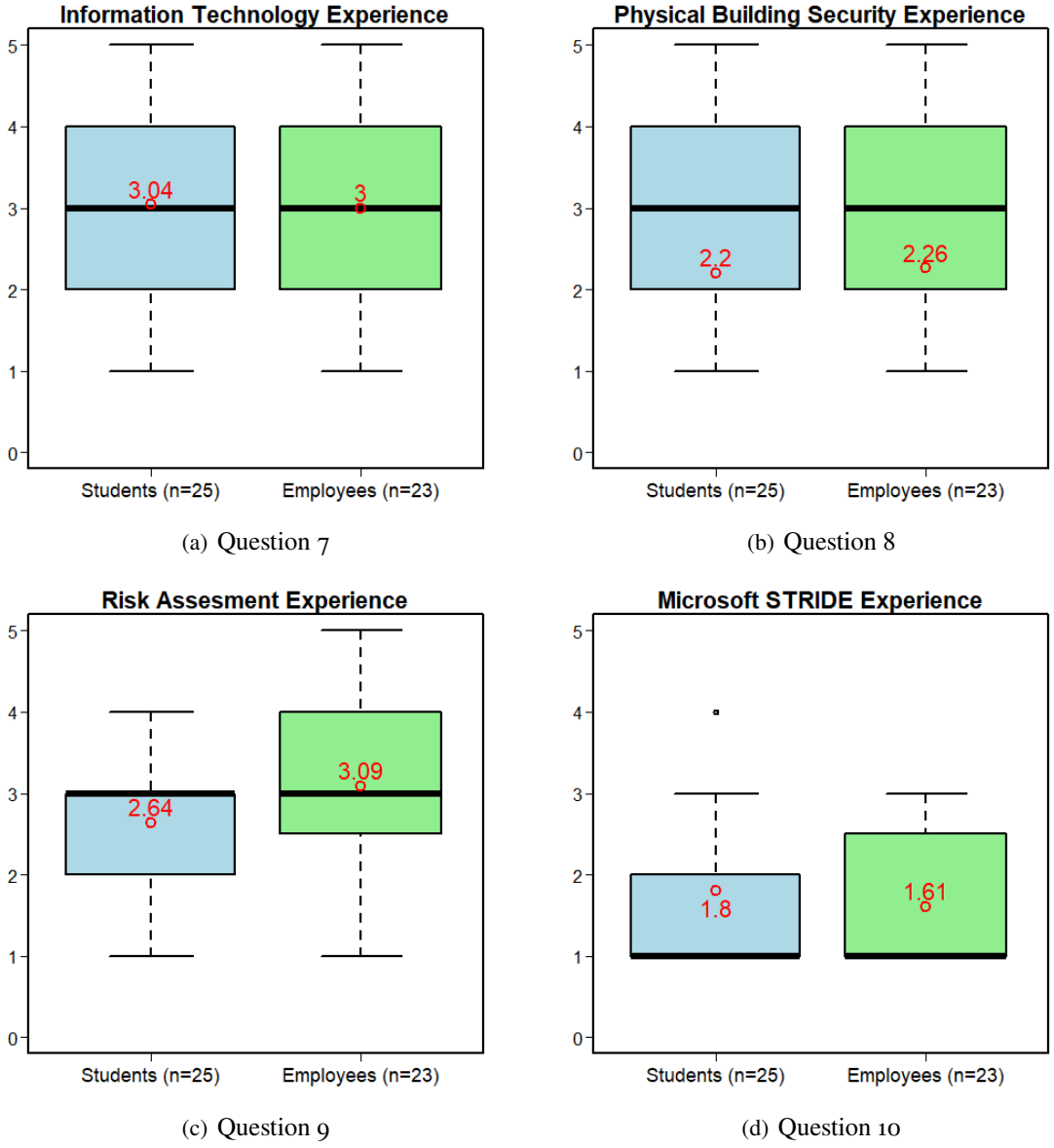
The last experiment took place in April 2019 as part of a professional training course for "Chief Data Officers" to allow an audience of 13 legal practitioners and lawyers to develop an awareness of cyber security risks and defences. All 13 post-task questionnaires were completed.

5.3 Analysis of Riskio Study Results

5.3.1 Pre-task Questionnaire (Players Background)

Players Backgrounds

Only two players, one from the employees' group and one from the students' group, have a professional certificate in cyber security in CISSP/CISM/CEH or other related qualifications. Ten of the students held an MSc or BSc in Cyber Security or Information Technology related degree, with only three of the employees' group having related degree qualification (see Figure 5.1).



(a) Question 7 (b) Question 8

(c) Question 9 (d) Question 10

Figure 5.1: Riskio Game Evaluation Questions 7 to 10 Players Background.

Figure 5.2 shows the answer to two background questions in questionnaire 1. ***Question 4*** - *How would you describe your level of expertise in cyber security?* Furthermore, ***Question 5*** - *How*

would you describe your level of knowledge in cyber attack trends? Both show the same IQR spread of data for both questions. However, in Question 4 on expertise in cyber security, the median for students of 4 was one point higher than 3 of employees. The students higher score is probably because of the student having a higher number of related degrees in information technology (see Appendix E for complete players background questionnaire).

(a) Students (n=25) (b) Employees (n=23)

Figure 5.2: Riskio Game Evaluation Question 4 (Level expertise in cyber security) & Question 5 (Cyber attack trends) Players Cyber Security Background.

5.3.2 Post Task Questionnaire

This section analyses the post-task questionnaire's responses to assess participants' perception of the Riskio game in increasing awareness in cyber security and evaluating if 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.

Figure 5.3 is the response to questions 1 to 13, which are specific about Riskio. Figure 5.4 is the response to the three generic questions about serious security games post-playing the game. See Appendix F for a complete list of questions from questionnaire 2.

The analysis has realigned the responses to 5 (which indicates the highest participant's perception). Then, an unpaired t-test to test for statistically significant differences (α set to 0.05) between students and employees' responses. The results are summarised in Table 5.2. Each question is reported as the question's perception variable (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 reported in bold. The average responses for each perception variable and the overall perception conclude the table.

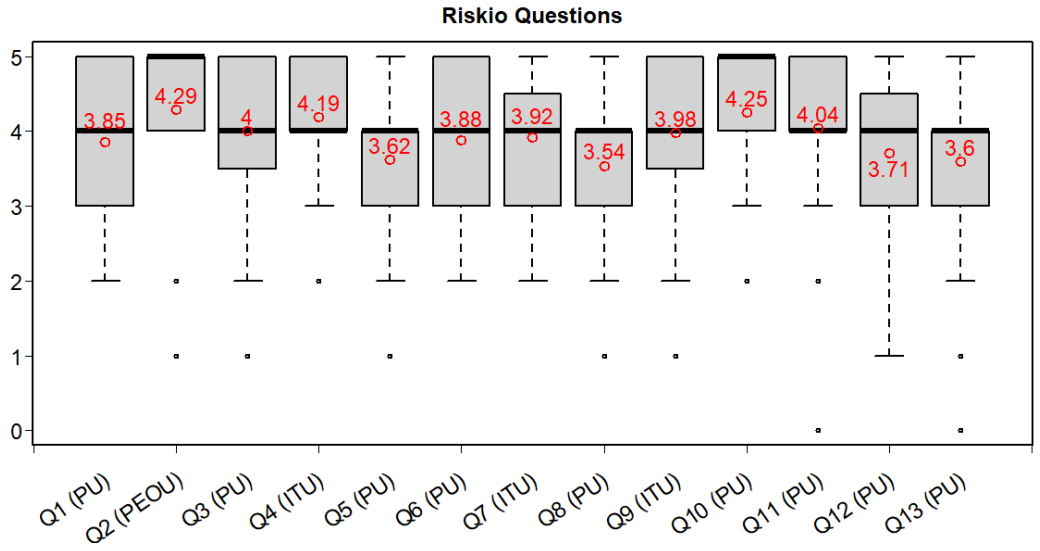


Figure 5.3: Riskio Game Evaluation All Post Task Questions (n=48).

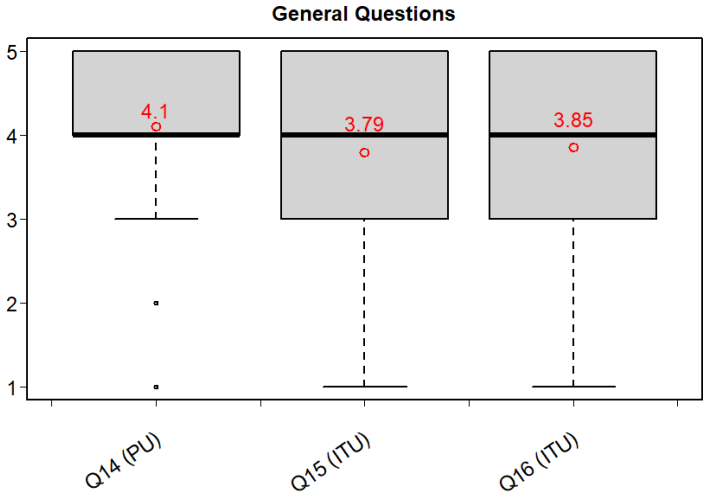


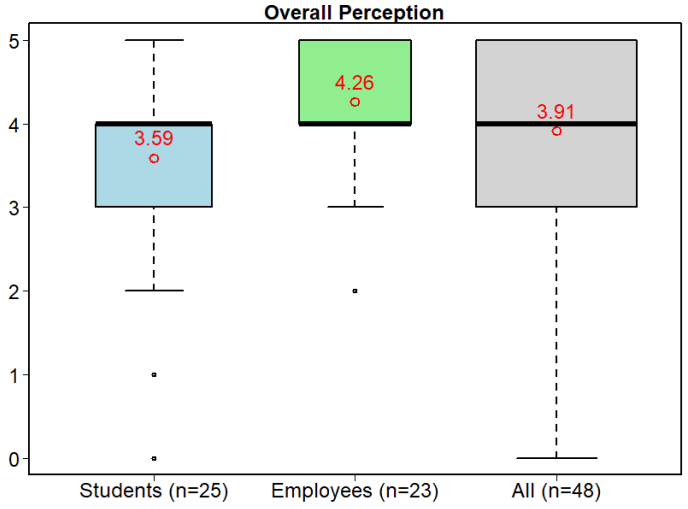
Figure 5.4: Riskio Game Evaluation Questions About Other Serious Security Games (n=48).

The following reports the analysis of the results, together with the outcomes of the feedback analysis, 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 Figure 5.5). Specifically, it emerged that the fun element was missing for the students: 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 use it during the gameplay like in other games such as monopoly*". In contrast, employees reported that "*We like the game as it was played*".

Table 5.2: Riskio Post-Game t-test of questionnaires responses (in bold statistically significant differences questions between Students & Employees).

Q. No	Type	Students Mean	Employees Mean	All Mean	All IQR	p-value	Hypothesis Test
Participants		(n=29)	(n=25)	(n=54)	(n=54)		
Questionnaires		(n=25)	(n=23)	(n=48)	(n=48)		
Q1	**PU**	**3.4**	**4.35**	3.85	3-5	**0.001467**	**False**
Q2	PEOU	4.2	4.39	4.29	4-5	0.5345	True
Q3	**PU**	**3.68**	**4.35**	4	3.5-5	**0.01284**	**False**
Q4	ITU	3.96	4.43	4.19	4-5	0.05709	True
Q5	**PU**	**3.24**	**4.04**	3.62	3-4	**0.008803**	**False**
Q6	**PU**	**3.48**	**4.3**	3.88	3-5	**0.001561**	**False**
Q7	**ITU**	**3.64**	**4.22**	3.92	3-4.5	**0.01325**	**False**
Q8	**PU**	**3.08**	**4.04**	3.54	3-4	**0.00184**	**False**
Q9	ITU	3.8	4.17	3.98	3.5-5	0.2354	True
Q10	**PU**	**3.96**	**4.57**	4.25	4-5	**0.02323**	**False**
Q11	**PU**	**3.68**	**4.43**	4.04	4-5	**0.009693**	**False**
Q12	**PU**	**3.32**	**4.13**	3.71	3-4.5	**0.006241**	**False**
Q13	**PU**	**3.12**	**4.13**	3.6	3-4	**0.002555**	**False**
Q14	PU	3.88	4.35	4.1	4-5	0.1267	True
Q15	ITU	3.6	4	3.79	3-5	0.2239	True
Q16	**ITU**	**3.56**	**4.17**	3.85	3-5	**0.0301**	**False**
	PU	**3.48**	**4.27**	3.86	3-5	**1.267e-01**	**False**
	ITU	**3.71**	**4.2**	3.95	3-5	**0.0001047**	**False**
	PEOU	4.2	4.39	4.29	4-5	0.5345	True
Total	All	**3.59**	**4.26**	3.91	3-5	**3.955e-19**	**False**



All Questions (16 questions)

- Students Mean 3.59
- Employees Mean 4.26
- All Mean 3.91
- p-value 3.955e-19

Comments: t-test no significant difference between students and employees - **False**

Figure 5.5: Riskio Game Evaluation Overall Perception.

Perceived Ease of Use (PEOU): Both employees' and students' have high confidence that the Riskio game mechanics and rules are easy to understand (see Figure 5.6). Some of the employees' who did know STRIDE reported that "*We were able to familiarise with the threats as the game proceeded and thanks to the feedback of our colleagues*".

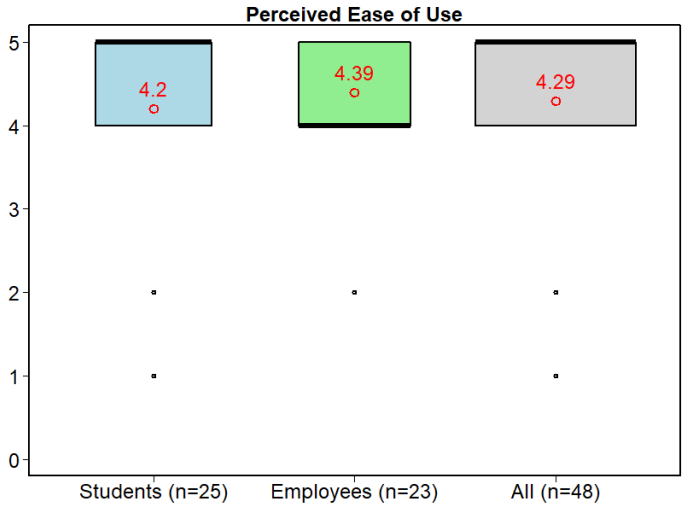


Figure 5.6: Riskio Game Evaluation Perceived Ease of Use (PEOU).

Question 2 (1 Question PEOU)

- Students Mean 4.2
- Employees Mean 4.39
- All Mean 4.29
- p-value 0.534474

Comments: t-test no significant difference between students and employees - **True**

Perceived Usefulness (PU): The perceived usefulness of the Riskio game in increasing awareness in cyber security is higher for employees than for students with statistical significance (see Figure 5.7). In particular, employees are more confident that the Riskio game is an effective solution to identifying cyber threats and more helpful in finding defences than students. Instead, students experienced difficulties 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*.

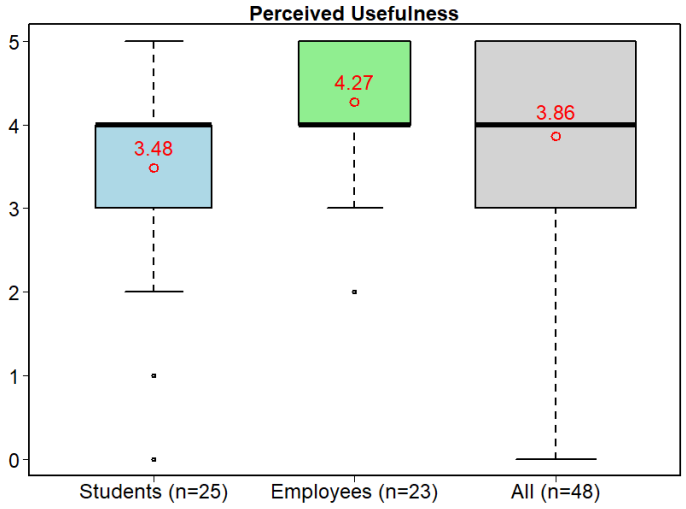


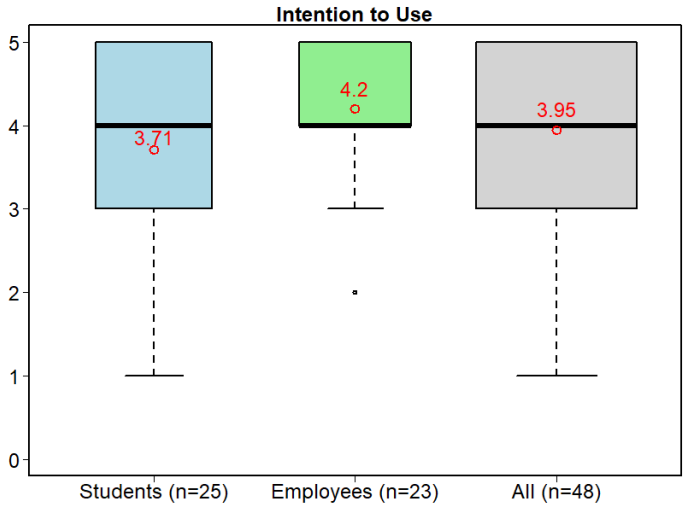
Figure 5.7: Riskio Game Evaluation Perceived Usefulness (PU).

Questions: 1, 3, 5, 6, 8, 10, 11, 12, 13, & 14 (10 Questions PU)

- Students Mean 3.48
- Employees Mean 4.27
- All Mean 3.86
- p-value 1.267e-1

Comments: t-test no significant difference between students and employees - **False**

Intention to Use (ITU): The intention to use the Riskio game to identify cyber defences in their organisation is higher for employees than for students (see Figure 5.8). Employees expressed higher intention to use the Riskio game to identify cyber defences in their organisations. The differences can be because they reported, "*We like the office diagram because we can relate this to our work environment*".



Question 4, 7, 9, 15, & 16 (5 Questions ITU)

- Students Mean 3.71
- Employees Mean 4.2
- All Mean 3.95
- p-value 0.0001047

Comments: t-test no significant difference between students and employees - **False**

Figure 5.8: Riskio Game Evaluation Intention to Use (ITU).

Summary by TAM, Figure 5.9, shows that although only one question, the IQR for PEOU was 3 to 4 with a median of 5, whereas both PU and ITU IQR was 3 to 5 with the same median of 4.

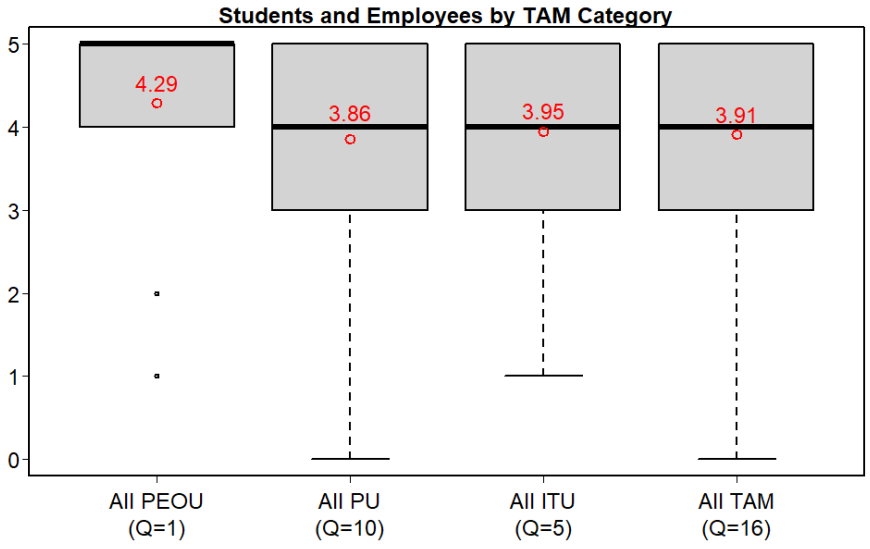


Figure 5.9: Riskio Game Evaluation Questions by TAM Category (n=48) (Q = Total Number by TAM).

5.3.3 Observations from Riskio Gameplay

The following are a list of key findings from the observations from the four experiments (see subsection 4.1.2) from the feedback of the games masters:

1. One group questioned in the pre-game tutorial why the use of Microsoft STRIDE as a threat model. Microsoft is not a good example, as they have many vulnerabilities in their software and constantly issuing patches. The participants agreed when the games master

explained in the tutorial that STRIDE is a governance threat model to help you elicit threats and categorise them.

2. The early version of game board University Office fees used term unknown to players and games masters, 'PDQ Machine' and game board updated to replace the word with 'Credit Card Machine'.
3. Games masters complained of difficulty awarding just one point for attack and defence. Rules changed to allow for up to three points (see Figure 4.14 for attack example and see Figure 4.15 for defence example).
4. Players were asked about the University Office Fees game board. All players, technical and non-technical, seemed to like this board, even when technical players showed network and data flow diagrams.
5. The players from work employees groups often started side conversations at the end of the round, discussing work-related issues to the game round just played.
6. It was agreed in a conversation between games masters after the first experiment that the players valued feedback using real-world examples of attacks and defences over theoretical examples.
7. Games masters were provided with a list for every attack card with a possible attack on the game board and a possible defence, see Appendix G as example Riskio Spoofing suit. However, games masters did not find this helpful to try and look at the list during gameplay.
8. Players preferred the feedback from the games master over awarding points for successful attack or defence, and awarding points was stopped, see observation 9.
9. Game masters were asked to record the cards played by the players and points awarded (see Figure 5.10). The games master found writing down and giving feedback challenging without disrupting the game's flow.

5.3.4 Summary differences between Students and Employees

Table 5.2 Riskio post-game questionnaire of the sixteen questions five was tested true for the null hypothesis (Q2, Q4, Q9, Q14 & Q15) that there was no difference between students and employees. However, eleven questions showed a significant statistical difference. The TAM model can describe the students and employees statistically different on the eleven questions. Nine questions were statistically different Perceived Usefulness (PU) (Q1, Q3, Q5, Q6, Q8, Q10, Q11, Q12 & Q13) Figure 5.7. The PU shows the exact median of 4 for students and employees. However, both have different IQR of students 3-4 and employees 4-5. However, students had a much more comprehensive range of answers and outliers. These differences are also confirmed in observations and questions where students have no reference or current experience of work-related cyber courses. Two questions were statistically different Intention to Use (ITU) (Q7 & Q16). The differences followed observational feedback comments where employees could see how the game could be used in a work context. Whereas students did not have the same work context and, although they enjoyed playing the game, did not have the same work context to evaluate the ITU.

Riskio

A Serious Game on Risk Management

Key to recording card played:

Attack Suit: S = Spoofing; T = Tampering; R= Repudiation; I = Information Disclosure D = Denial of Service; E = Elevation of Privilege

Card: Number card: 2; to 10; J = Jack; Q = Queen; K = King; A = Ace

Example: Round 0

			Player No Card(s) Played					
Round No	**Point Type**	**Games Master**	**1**	**2**	**3**	**4**	**5**	**6**
0	Attack Point		1 D2					
	Defence Point			1 D2/DA	0 DJ	0 DQ	1 D7	1 D7
	Bonus Point	I2	0	1	1	0	1	0
1	Attack Point							
	Defence Point							
	Bonus Point							
2	Attack Point							
	Defence Point							
	Bonus Point							

Figure 5.10: Extract Riskio Game Scoring Sheet.

In summary, the difference between students and employees for Perceived Usefulness (PU) and Intention to Use (ITU) from observation and talking to the groups is because the students do not have the same work experience as the employee's group and do not have the same context of how useful at work to play serious games to complement current work-related cyber training.

5.4 Threats to Validity

This section discusses the study's validity's main threats: construct, reliability, internal and external validity (Wohlin et al., 2012). The four experiments where data was collected were employees' part of staff induction, the second students as part of MSc, the third and fourth were part of a professional training course. Participation was voluntary, and both background questionnaire 1 (see Appendix E) and post-game questionnaire 2 (see Appendix F) were anonymous and impossible to link the responses between the two questionnaires.

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 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 eleven questions for Perceived Usefulness and four questions for Intention to Use but only one question for Perceived Ease of Use. Therefore, we are reasonably confident that the questionnaire measures PU and ITU, while for PEOU, we cannot conclude the results.

Reliability. Reliability is the aspect concerned with the extent to which the data and the analysis are dependent on the specific researchers. The participants were required to have the same presentation about the Riskio game, including an overview of the STRIDE threat model before playing the game and answering the questionnaire. The identified risk is that the presentation may vary in content and delivery even from the same presenter and affect the participants' answers. Mitigated this by using the same presentation and supporting examples to ensure this was consistent.

Internal validity. Internal validity concerns 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 using the author and supervisors of this paper as game masters. The participants who played the game with the games masters might have felt obliged to rate the game's perceptions more highly. The risk was mitigated by clarifying that the participant's responses would be anonymous at the beginning of the study. Another aspect that might have biased the results is the level of expertise of the game master. For example, the participants who played the game with PhD students as game masters might have had a lower perception of the game than the other participants. The PhD students were trained to be game masters by playing the game with them several times to mitigate the threat of inconsistency in the games master.

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 the survey. A possible threat could have been to select the wrong people to participate in the experiments. However, this was not the case because we have selected participants matching our target audience from the game. We mitigated this threat by using the university fees office board that create opportunities to think about realistic attack scenarios and defensive strategies.

5.5 Discussion and Reflections

5.5.1 Pedagogical Design

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 2.5) prove the benefits of using (tabletop) games for cyber security education, as the landscape of cyber security threats keeps changing over time. The main challenge for the game design was to create game content, i.e., the cards and the board that can be easily adapted to a different audience (either operative, administrative or technical) and play scenarios (either real-world business scenarios or technical drawings). To this aim, the following trade-offs were identified that could also be pursued to design other serious security games.

5.5.2 Game Design

Game cards: The card design process started by looking at the proposals of the EoP game. However, playing EoP with original game cards do not make the players critically think about the threats on the attack cards, hindering the active learning environment. For example, card contents like "*An Attacker can reflect input to a user, like cross-site scripting"* will not be understood by a non-technical audience. On the other hand, it does not allow the players to point out that the card may lead to a cross-site scripting attack (as already written there!). To this aim, the formulated card contents do not provide the answer. For example, "*An attacker sends email targeting a specific user*", which allows players to elicit attacks including, e.g. 'Spear Phishing' or "Whaling' techniques, and be widely understood by all types of audience.

Although the Riskio card design does not lead to a unique set of correct attacks for each card, experience with playing the game has confirmed that players are eager to show their knowledge. If the player acting as the attacker does not mention a potential attacking technique based on 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 a different audience.

Game boards: The design of the game board is fundamental to allow players to experiment with a variety of attacking and defending scenarios. As the designed cards encompass both software, physical and social engineering techniques, it was realised that a board representing cyber-physical gameplay was the most fitting choice. The University fee office board (Figure 4.9) was positively rated by the players, both for the ease of identifying attack scenarios and creating multiple plotlines (e.g. exploiting admin personnel, vulnerable online service, or lack of physical security).

However, based on the feedback provided during experiments, it was realised that some modifications to the board might be necessary according to the audience. For example, to

facilitate an audience with no experience in threat identification, students' suggested that we annotate the assets on the board with the applicable STRIDE threat categories (see Figure 5.11). 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 Figure 4.10). For students who wanted a random selection of STRIDE suit alternative game board where you roll a dice (see Figure 5.12).

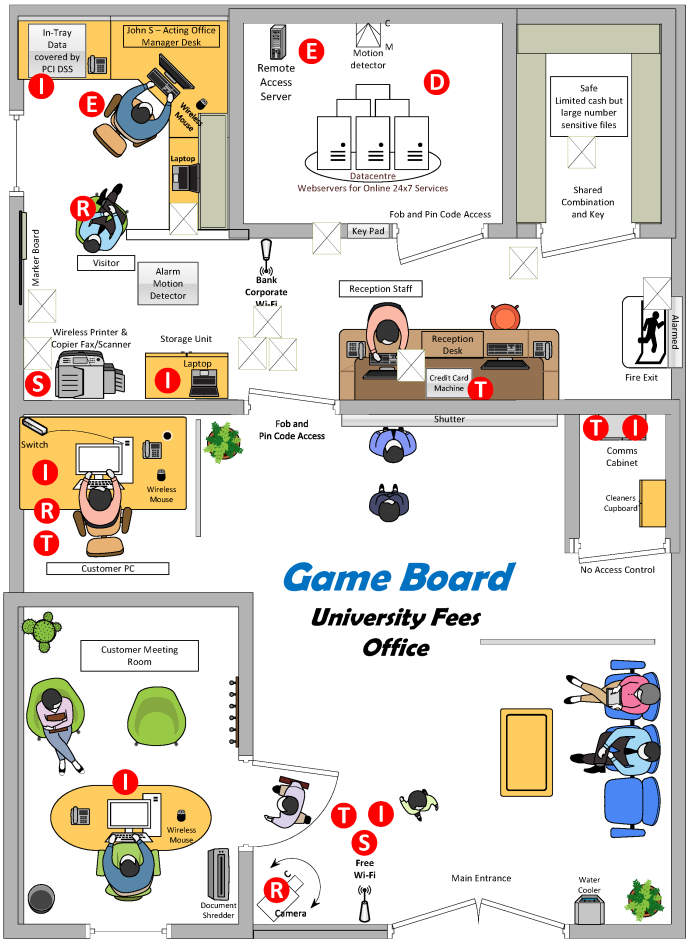


Figure 5.11: Riskio Game Board: Annotated Office Diagram.

STRIDE Annotated Diagram

Threats are mapped on the office diagram using the Microsoft STRIDE threat categories annotated by the first character of the STRIDE category

Card Graphic Design and Illustration: The graphic design, illustration, and size and quality of paper used to print the cards significantly affects the players' initial reception. After this, we hired a professional designer to design the cards. Players constantly repeated that they felt like playing an actual card game.

5.5.3 Game Mechanics

Game Mechanics Trade-offs: The game was evaluated with different gameplay options to allow the players to experiment with both attacking and defending phases in the following scenarios:

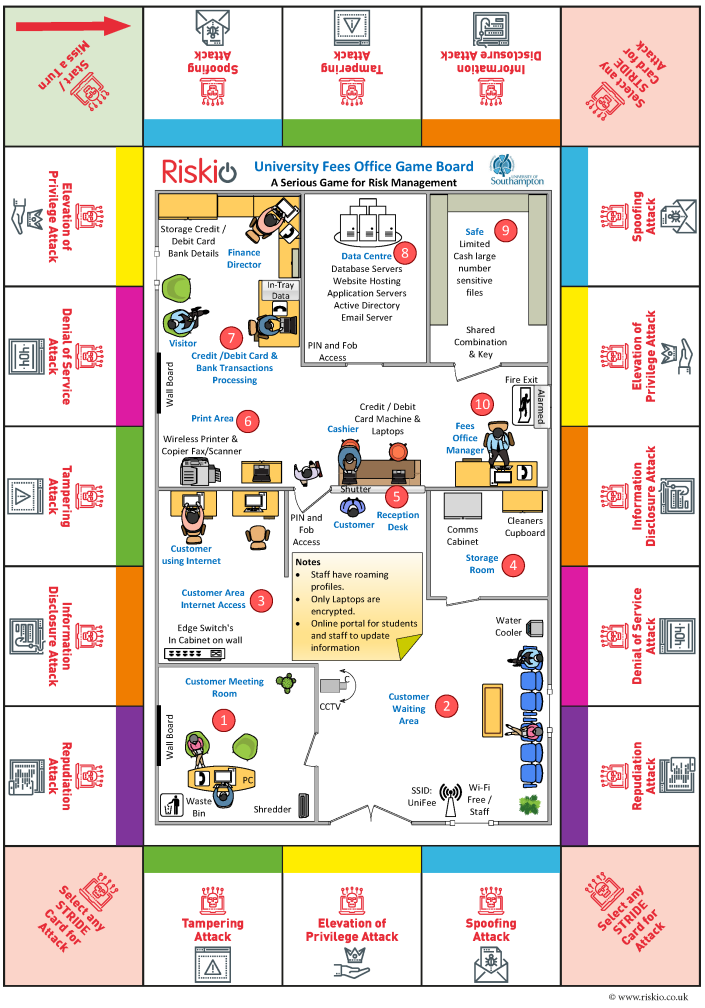


Figure 5.12: Riskio Game Board: Alternative Office Diagram V2.

Random Selection of STRIDE Suit

Players roll a dice to move around the game board, and the square they land on will be the STRIDE suit they use for the attack

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

The first option led the gameplay 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 4.5, the final choice was the third option. The option where players took turns to attack and then defend proved the design 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 broader 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, fun, and entertainment. 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, it was realised from the experiments that the game master should be "fading in the background" when the players become more knowledgeable, thus avoiding the players perceiving the gameplay as a lecture.

Scoring: From the experiments, it was noted from feedback that players were not interested in the scoring phase of the game.

Risk Management Process: The real-life complexity of security decision making encompasses, among others, risk prioritisation and security expenditure. Budget limitations lead to a trade-off in choosing the highest risks to mitigate and the appropriate defences and countermeasures. C-level people frequently make decisions that may not fully comprehend security risks: the Riskio game could 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, the game will evaluate the introduction of a new game phase. The game master prioritises the threats identified by the players and then lets the players identify defences within a given budget. Differently from other games (Frey et al., 2017; Williams et al., 2010), based on thinking, the players should focus more on understanding the role of threat countermeasures rather than risk prioritisation, for which each organisation may follow different approaches.

5.5.4 Riskio Limitations

The Riskio game is very adaptable. You can create new game boards from fictional to real-world by the team playing with a game based on real organisational context. The game boards could be based on an office like a fictional University Fees Office, or the players could create a network or data flow diagram, similar to the EoP game. You can also change the cards, currently based on the Microsoft STRIDE threat model but could change, for example, to use DREAD. However, there are two fundamental limitations of the Riskio game. The first is relying on an experienced cyber professional to act as the games master. An alternative is to turn Riskio into an online game and use a pedagogical agent. The agent to improve and enhance the learnability of the serious game (Atorf et al., 2019). The second limitation is the defence stage has no concept of cost or effort in defences. Costs proved in early development to be more challenging to include in early testing and development of the game because of the wide range of possible attacks. It was noted in playing experiments that players tended to select more complex technical options. For example Intrusion Detection System (IDS) to prevent phishing attacks over user training. Further work on Riskio needs to be done not only to include costs of defences but, as in the IDS example, cost and effort of deployment and maintenance of any defence solution. However, only one game was found that had the concept of defence costs and a budget, Decisions & Disruptions, see Table 5.3.

Table 5.3: Serious Games: Have Defending with Costs and Budget.

Game	Defending?	Costs?	Budget?
2.5.5 CyberCIEGE	Yes	No	No
2.5.6 PERSUADED	Yes	No	No
2.5.8 Decisions & Disruptions	Yes	Yes	Yes
2.5.11 Cryptomancer	Yes	No	No
2.5.12 Cyber Threat Defender	Yes	No	No
2.5.13 Exploit!	Yes	No	No
2.5.14 Operation Digital Chameleon	Yes	No	No
2.5.16 Social Engineering Requirements Game	Yes	No	No
2.5.17 Play2Prepare	Yes	No	No
2.5.19 Crypto Go	Yes	No	No
2.5.21 SherLOCKED	Yes	No	No

5.6 Conclusion - Serious Games Design

Chapter 4 showed how the game called Riskio was developed. In Chapter 5, the game was evaluated, and although the game proved successful with the target players, how can one design serious cyber games that meet learning objectives and are not just fun games to play? We still need a pedagogical model to design serious games for awareness and education. Chapter 6 explores the suitability of current published serious cyber games design models and uses Riskio to evaluate them.

Part III

Pedagogical Model to Design Serious Cyber Games

Chapter 6

Pedagogical Serious Games Design

This chapter attempts to apply a current published serious games assessment model to the Riskio game to find if using the model achieves stated objectives in designing serious cyber games. Section 6.1 reviews the design models to select one for an illustrative case study to test the model's efficacy. Section 6.2 uses the Riskio games to assess the model. Section 6.3 concludes if to adapt an existing design model or create a new model.

6.1 Serious Games Design Assessment Models

There is consensus on the benefits of the potential use of gamification. However, there is still a lack of pedagogical driven methodologies and tools to support the analysis of serious games (Arnab et al., 2015). The first step was to select a published model to apply to Riskio using the model to verify that the serious game meets the learning objectives. Three models were considered, the Game Object Model (GOM) (Amory, 2007), Serious Game Design Assessment Framework (SGDAF) (Mitgutsch and Alvarado, 2012) and LM-GM Model (Arnab et al., 2015).

6.1.1 GOM Model

The Game Object Model (GOM) model is based on a constructivist theoretical framework to support serious educational games development (see Figure 6.1). The five components of the GOM model does not show how they influence each other (Arnab et al., 2015) and how the components link to the game mechanics and, therefore, the serious game learning objectives. The GOM is a high-level model and will not assist in selecting game mechanics to achieve serious game objectives. Therefore, the GOM model was excluded from the next stage testing model with the Riskio game.

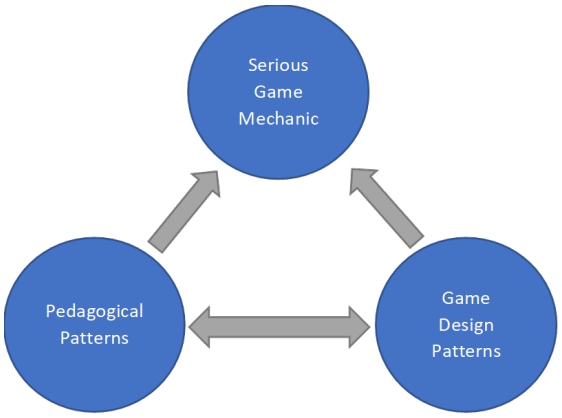


Figure 6.1: Game Object Model (GOM) Model (Amory, 2007).

6.1.2 SGDAF Model

The Serious Game Design Assessment Framework (SGDAF) model see Figure 6.2 requires going through all the seven steps: 1) Purpose; 2) Content / Information; 3) Mechanic; 4) Fiction / Narrative; 5) Aesthetics Graphics; 6) Framing, and 7) Cohesiveness & Coherence of Game. While applying the SGDAF model to Riskio, many elements were practical when reviewing against Riskio lessons learnt in the game design (see Section 4.1). For example, in step five, the aesthetics and graphics in so far, the quality of cards affected the players' enjoyment of the game. Early versions of the game did not have professionally designed and printed cards noted from players comments in an earlier version of Riskio. The quality of the game materials is an example where design is called out design (step 5, aesthetics & graphics) the SGDAF Model but not in the GOM Model. However, SGDAF had a similar problem to the GOM model as in step 3. The model provides no mechanism to map the game mechanics to the learning objectives.

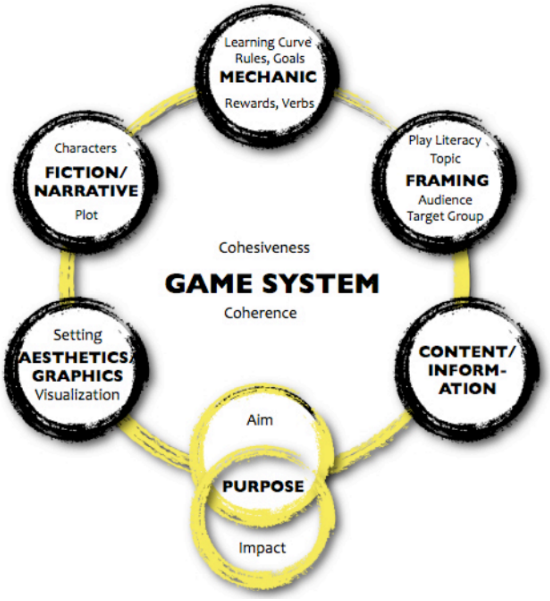


Figure 6.2: Serious Game Design Assessment Framework (SGDAF) Model (Mitgutsch and Alvarado, 2012).

6.1.3 LM-GM Model

The LM-GM Model (Lim et al., 2015), see Figure 6.3, was created on the assumption that the fundamental design of serious games relies on the translation of learning goals into the mechanical element of the gameplay (Arnab et al., 2015). The LM-GM was created to overcome the missing descriptive relationship between learning mechanics and game mechanics. The LM-GM Model also maps the game mechanics to Bloomś ordered thinking skills Table 6.1. The initial review of the LM-GM Model against the components identified in the literature review showed that the LM-GM model could cover all the areas identified in the review (see Figure 2.32).

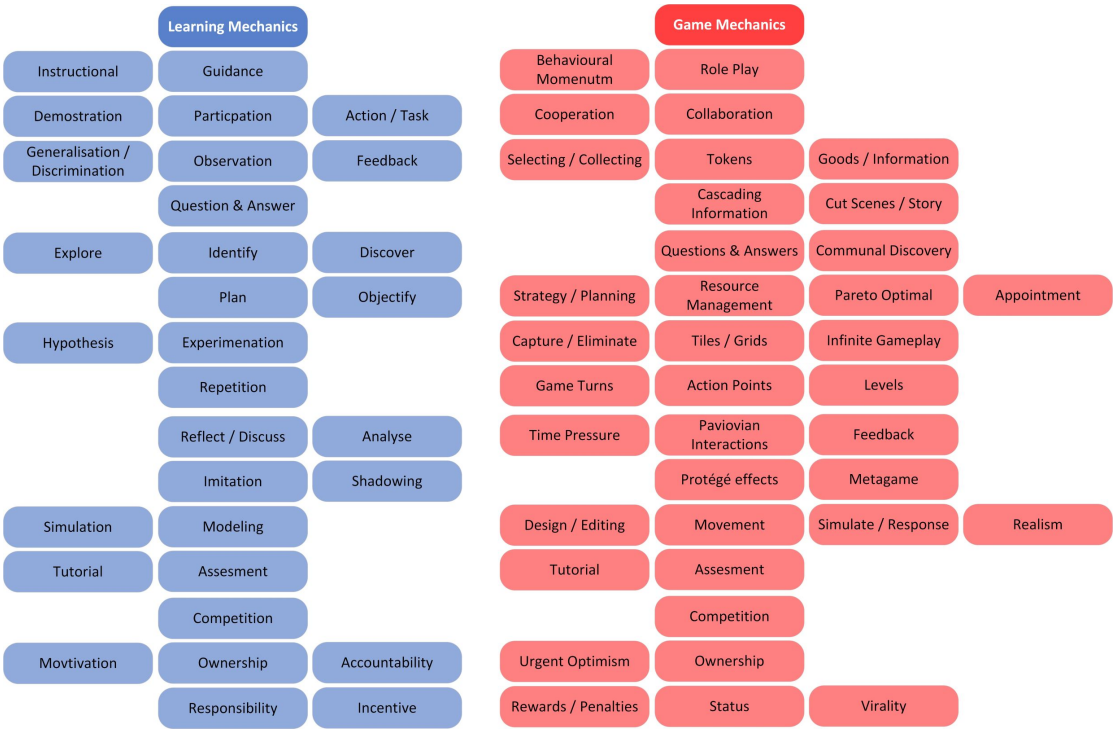


Figure 6.3: LM-GM Model Mapping Learning Mechanics to Games Mechanics (Lim et al., 2015).

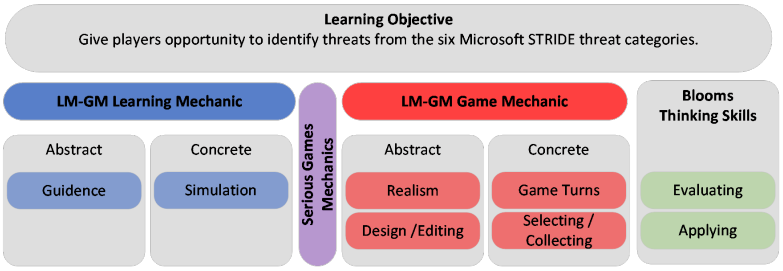


Figure 6.4: LM-GM Model: Links between Model Components.

6.1.4 Evaluation of Models

Arnab et al. (2015) publication was shared with supervisors and used as a base for conversation, including mapping Riskio using the LM-GM model to the Riskio gameplay (see Figure 6.7) and other possible design models GOM and SGDAF.3

We decided not to evaluate the models with students using the same methodology as Arnab et al. (2015) by getting students to evaluate games using the models to analyse the gameplay. The Arnab et al. experiment 1 required the participants first to play a serious game, complete a pre-questionnaire, then receive a presentation on the model, then use the model to map the gameplay of the game they just played finally complete a post-questionnaire. This process was repeated for the second model with a different game for comparison. We were concerned about the effort required, output quality, and issues found. For example, out of ten participants who used this process in one Arnab experiment, three were unmindful or careless. We decided to use an alternative method for evaluation by creating an illustrative case study. The reason for this from our experience was the time required to learn the model and map the gameplay. Figure 6.4 using the LM-GM model, as an example, to show using one learning objective from Riskio game *"Give players opportunity to identify threats from the six Microsoft STRIDE threat categories"*. The complex relationship of just one learning objective in the many-to-many relationship between abstract and concrete of the LM-GM learning mechanics and LM-GM game mechanics can be seen.

6.1.5 The Conclusions

Both the GOM Model and the SGDAF Model were rejected because of the lack of methodology of linking game mechanics back to the learning mechanics and the serious educational objectives of a serious cyber game. The LM-GM Model was selected for the next stage to mapped Riskio gameplay to verify the model and test with selected University staff who understand pedagogical frameworks to verify the proposed LM-GM Model using .

6.2 Illustrative Case Study using LM-GM Model

This section uses Riskio as an illustrative case study to test the efficacy of the LM-GM Model. Figure 6.5 depicts the components of the LM-GM model and is represented by the Learning Mechanics (LMs), the nodes to the left of the model in blue and the Games Mechanics (GMs), the nodes to the right of the model in red. The nodes' right and left are leaf's related LMs and GMs to the respective node.

The model is descriptive rather than prescriptive and allows users to relate learning mechanics to game mechanics. The abstract game elements (Game Mechanics) can be mapped many-to-one to the concrete game elements, and single-game Learning objectives can be achieved through

Figure 6.5: LM-GM Model Node and Leaf (Lim et al., 2015).

different learning activities (Learning Mechanics). A single game dynamic/learning objective can be achieved through several game mechanics.

Bloom's theory (Bloom, 1956), is a simplified framework/classification, see Table 6.1. The commonly found game mechanics to learning mechanism can be linked back to Bloom's taxonomy: Retention; Understanding; Applying; Analysing; Evaluating; and Creating. The skills are ordered from lower-order thinking skills to higher-order thinking skills.

Using the LM-GM model to test the evaluation of the Riskio game, it took several hours to refine the evaluated model before it was to an acceptable level. Arnab et al. (2014) tested the LM-GM model with a second model to evaluate how effective the models were at enabling users to analyse the game. Three players responses were ignored for analysis from the ten participants responses as answers to questions on a scale of 1 to 5 were unmindful or careless. The complex relationship with many-to-many between LMs to GMs and many-to-one from abstract to concrete could be one of the reasons for the lack of attention from the three of ten participants (see Figure 6.4).

In Figure 6.6 is the Riskio serious gameplay has been mapped from the LM-GM model. In Figure 6.7, it is mapped back to Riskio gameplay.

The following issues were identified using the LM-GM to identify the game mechanics to deliver the learning objectives:

1. It is very time consuming to create the LM-GM model for Riskio, with revisions taking considerable time

Table 6.1: Blooms Taxonomy Mapped to LM-GM Model.

Learning Mechanic (LMs)	Thinking Skills	Game Mechanics (GMs)	HOTS to LOTS
• Accountability • Ownership • Planning • Responsibility	CREATING	• Design/Editing • Infinite gameplay • Ownership • Planning • Protégé effect • Status • Strategy/planning • Tiles/grids	**High Order Thinking Skills**
• Assessment • Collaboration • Hypothesis • Incentive • Motivation • Reflect/Discuss	EVALUATING	• Action Points • Assessment • Collaboration • Communal Discovery • Game Turns • Pareto Optimal • Resource Management • Rewards Programme • Urgent Optimisation	
• Analyse • Experimentation • Feedback • Identify • Observation • Shadowing	ANALYSING	• Feedback • Meta-game • Realism	
• Action/Task • Competition • Cooperation • Demonstration • Imitation • Simulation	APPLYING	• Capture/Elimination • Competition • Cooperation • Movement • Progression • Selecting/Collecting • Simulate/Response • Time Pressure	
• Objectify • Participation • Questions and Answers • Tutorial	UNDERSTANDING	• Appointment • Cascading Information • Questions and Answers • Role-play • Tutorial	
• Discover • Explore • Generalisation • Guidance • Instructional • Repetition	RETENTION	• Behavioural Momentum • Cut Scenes/Story • Goods/Information • Pavlovian Interactions • Tokens • Virality	**Low Order Thinking Skills**

2. Not clear how the game mechanics translate into the actual gameplay mechanics as stated by the categories in the abstract. For example, 'Tokens' does not state how they are used.

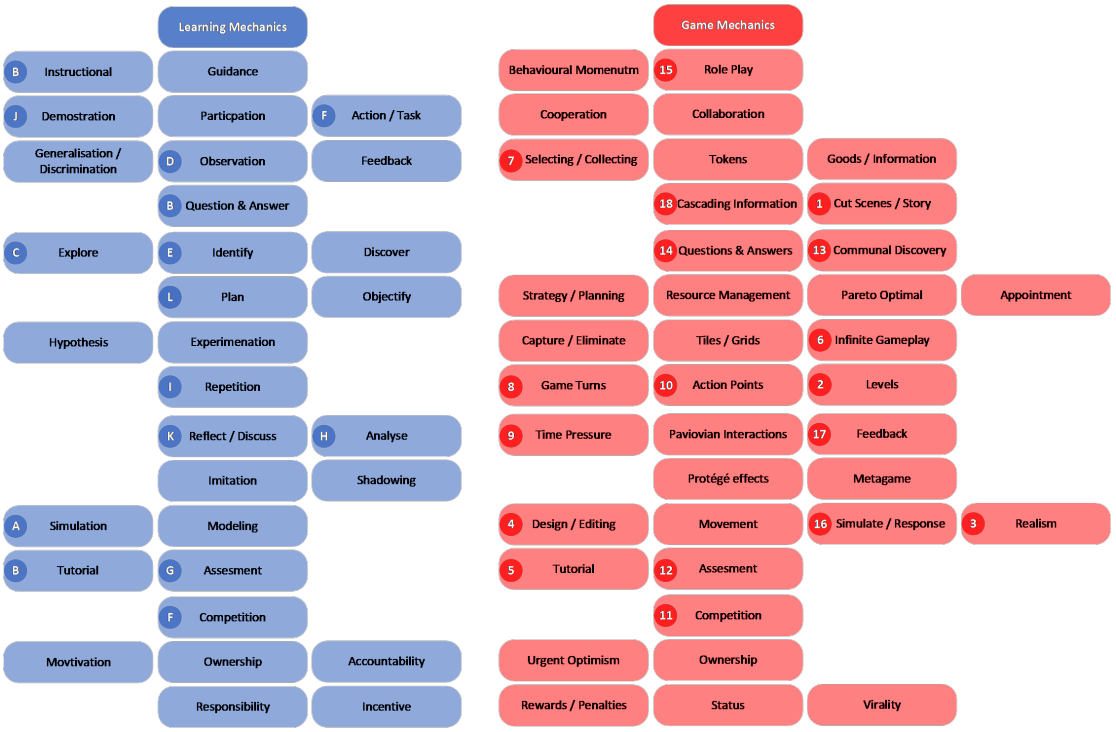


Figure 6.6: LM-GM Model Mapped to Riskio Gameplay.

3. The game mechanics in the model may have multiple ways to be used in the gameplay, but not all will deliver the learning objective

4. The model does not enable the selection of mechanics based on cognitive principles to meet target players motivations

5. There is no step-by-step guide to the creation of serious games

6. No consideration in the design to the target players requirements for learning which may be different

6.3 Conclusion Develop Current Model or Create New Model?

The creation of the game Riskio gameplay mapped to the LM-GM model took considerable time. It required concerted effort to create the map going through several iterations, following the evidence in testing the LM-GM Model in the Arnab study (Arnab et al., 2015). Out of ten participants using the LM-GM model, three were unmindful or careless. The LM-GM model does not link or consider some critical objectives for the pedagogical model found in the literature review, see Section 2.13. For example, objective 1 does not consider players motivation. The next stage in Chapter 7 proposes creating a new pedagogical model to design serious cyber games rather than develop an existing model.

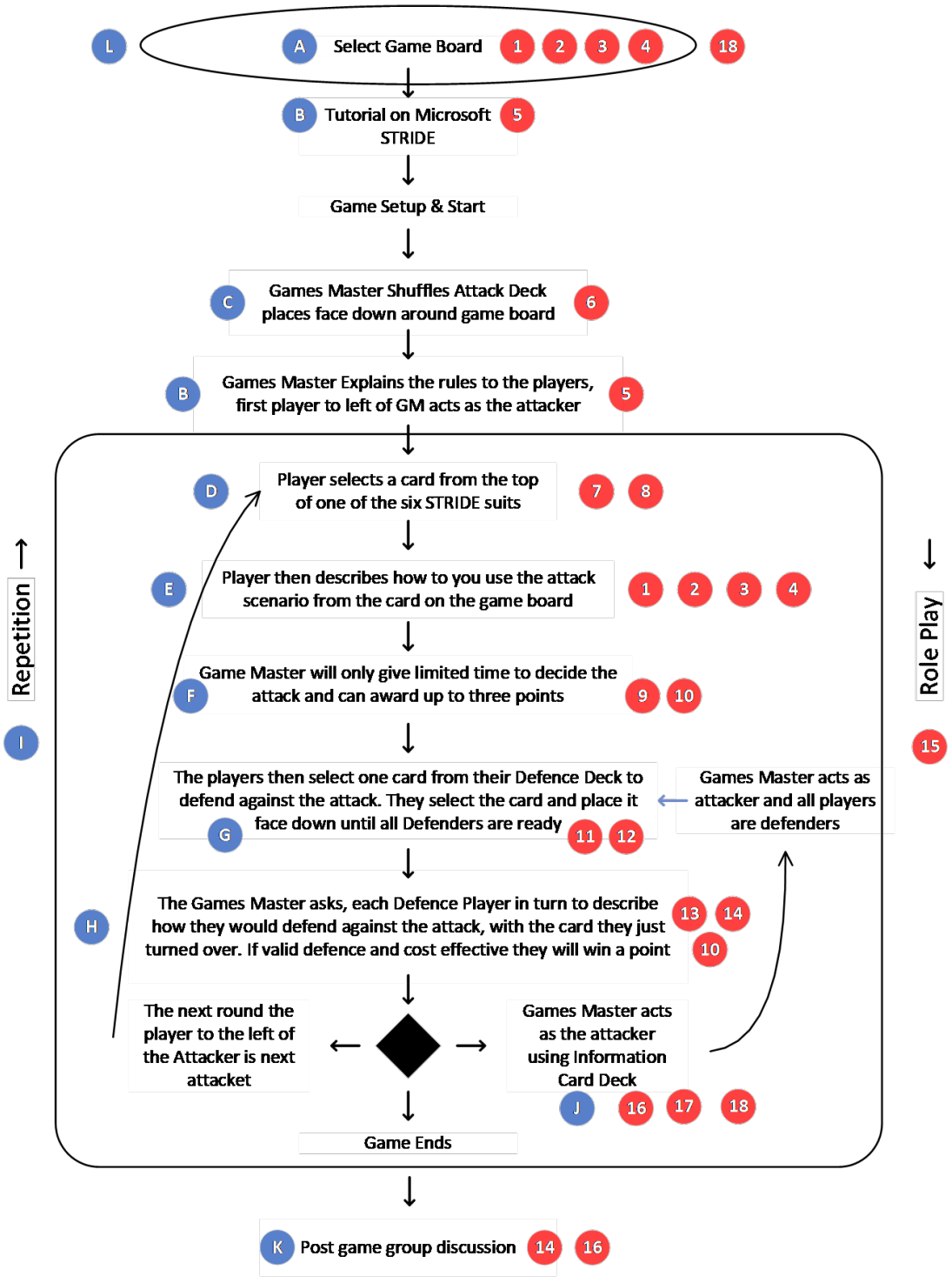


Figure 6.7: Riskio Gameplay Mapped to LM-GM Model.

Chapter 7

Proposed New Serious Cyber Games Design Model

The MOTENS model, see Figure 7.3, was created based on the gaps identified in the current games for pedagogical for the design of serious games for cyber security awareness and education and experience of lessons learnt from the creation of Riskio. The model is designed for serious cyber games rather than other types of serious games for education. Section 7.1 explains the supporting theory for Constructivist Learning Environments (CLE). Section 7.2 explains the process to create the new model. Section 7.3 explains the MOTENS model and links it to game mechanics and pedagogical theory. Section 7.4 is an illustrative case study to test MOTENS with people involved in serious games design. Section 7.5 is a comparative case study targeting students who are designing or interested in designing serious cyber games. Section 7.6 concludes with a summary of gaps the new MOTENS model has improved, as identified in Section 2.12.

7.1 Theory Learning Environments

We reviewed several models (GOM, SGDAF, and LM-GM) for serious games analysis and design that provided some valuable interpretations and limitations offered by the design and evaluation of serious games. However, these models focus primarily on high-level aspects and requirements. They do not help understand how such high-level requirements can be concretely satisfied (Carvalho et al., 2015) and help design a serious game. Carvalho et al. (2015) propose a new model of how a serious game connects educational and entertainment, high-level objectives with low-level game components. The model, named Activity Theory-based Model of Serious Games (ATMSG), is based on concepts of activity theory (Jonassen and Rohrer-Murphy, 1999). However, the ATMSG model is used to analyse serious games to understand better how learning takes place in the game and does not explain how you can use the model to create a serious game and only used for conceptual design.

In Section 3.2 we selected constructivism principles to be used to design the game learning environment, and activity theory is very consonant with those of constructivism. Jonassen and Rohrer-Murphy (1999) argue that for Constructivist Learning Environments (CLE) that activity theory provides an appropriate framework for analysing needs, tasks, and outcomes for designing CLEs. For the new model to create and design serious cyber games, we selected to use activity theory which is based on activity system (Engeström, 2015) a model of which is depicted as a triangle in Figure 7.1.

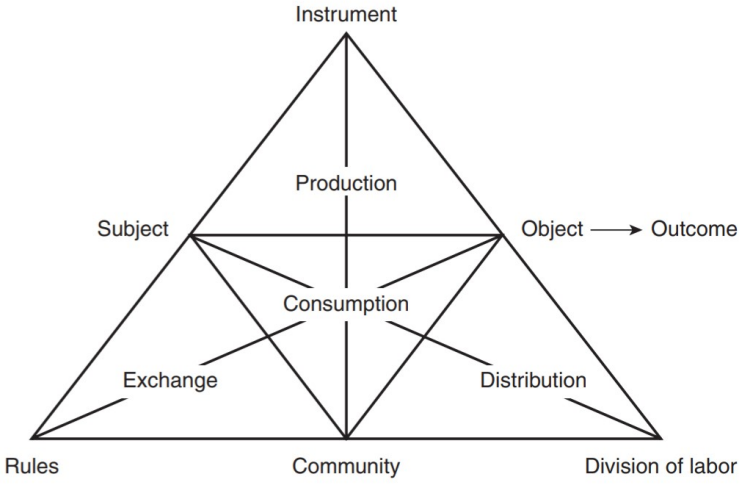


Figure 7.1: The structure of human activity (Engeström, 2015).

The model suggests analysing the multitude of relations within the triangular structure of activity. However, the essential task is the systemic review of the whole, not just separate connections. In Figure 7.2 an example of two people playing chess using Engeström's triangular heuristic (Engeström, 2015). The game elements (chess pieces) and rules have been historically produced through different activities. The players transform the gameplay object's towards the activity's outcome (Vermeulen et al., 2016).

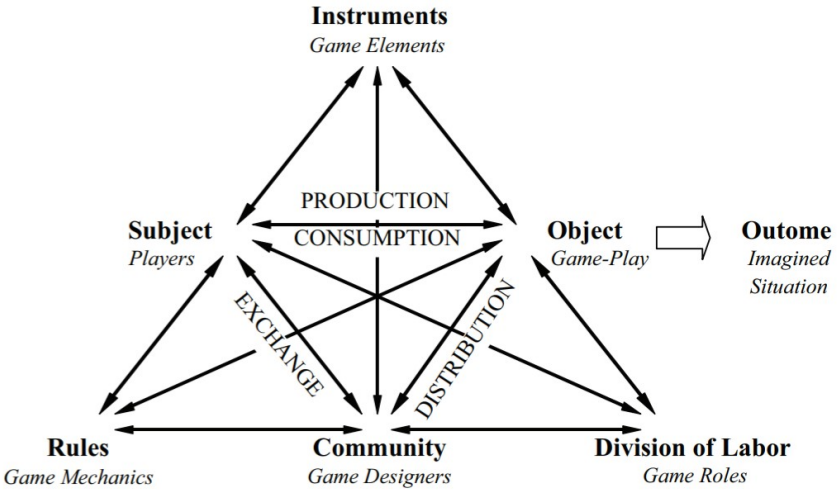


Figure 7.2: Game activity system (Vermeulen et al., 2016).

For describing the components and their relationships in the model is described in the activity theory in six steps in the CLE, (see Appendix H, applying activity theory six steps) for activities and questions for clarifying the purpose of the activity system (Jonassen and Rohrer-Murphy, 1999). In summary, the six steps to the activity system:

Step One: Clarify the purpose of the activity system. What are participants' goals and motives? What are their expectations about the outcome?
Step Two: Analyse the Activity System. The outcomes of this step will describe all aspects of the problem will be modelled in the CLE.
Step Three: Analyse the Activity Structure. The outcomes of this stage of any activity analysis will be a description of the activities, actions, and operations that are required to solve the problem in the CLE.
Step Four: Analyse Tools and Mediators. What tools might be used in this activity?, What formal or informal rules, laws, or assumptions? Who traditionally has assumed the various roles?
Step Five: Analysing the Context. The outcomes of these actions will describe the problem context that is modelled in the CLE.
Step Six: Analysing Activity System Dynamics. This is the step where you link the components of the CLE. See Figure 7.1 how all components link to achieve the outcome.

7.2 New Model Design Process

The conclusion of the review of current serious games models concluded with the decision to create a new pedagogical model (Section 6.3). It was decided to create a new model and not develop a new model based on one model but use the best ideas from all the models and add missing features. Riskio lessons learnt from the creation of the game were used to inform the design of the new pedagogical model for serious cyber games using Engeström's activity model, see Figure 7.1 and Figure 7.2.

7.2.1 Serious Games Design using Engeström's activity model

This section explains the Engeström's activity model using the Riskio game as an example.

Rules (Game Mechanics):

Game design must allow for changes to meet subject (players) requirements. For example, in Riskio, students wanted a random selection of STRIDE suit, whereas employees wished to select the suit (see game design subsection 5.5.2).

Subject (Players):

There was a difference between subjects (players) where students wanted more game-like play over employees. For example, students wanted to have a game board where they threw dice

to move around. Selection of instruments (game elements) must take into account subject (players) requirements (see example alternative game board Figure 5.12).

Instrument (Game Elements):

You can't assume that players have all the same knowledge. When playing Riskio using the EoP Game rule of using the 'EoP suit' as a 'Trump Cards', not all the players knew of this game concept. This option using trump card was used in "Experiment 1: October 2018", see Section 4.1.

The game elements for serious cyber games must be based on industry standards. For example, defences NCSC cyber essentials and for attack OWASP top 10 most critical web application security risks. This will improve relationship between subject (players) and instruments (game elements), see Figure 7.2.

Division of labour (Game Roles):

In testing Riskio, we tried to separate attacking and defending roles into two sessions. This option of two separate sessions was only used in "Experiment 2: October 2018", see Section 4.1. This did not work and confused the players. The best option was to have an attack then the defence as this improved the relationship between subjects (players) and the instruments (game elements). One player attacking (players taking turns) then all other playing defending enhanced the object and outcome as players understood the relationship between attack and defence (see Figure 7.2).

Object (Gameplay):

Players preferred feedback from games master over the awarding of points. Feedback is essential, and where the game does not have a game master, the design must include the option of giving players feedback (see subsection 5.3.3 list item 8).

Community (Game Designers):

The questions used in attacks should not be prescriptive so that players use lower-order thinking skills of remembering. The game designers should create fictional simulations to get players to use higher-order thinking skills, see Table 6.1. For example, Riskio attack deck card, 10 of Spoofing. "An attacker sends an email targeting a specific user". The question does not state phishing attack but tries to get the player to think about what type of attack and how the attacker obtained the information (see Riskio Spoofing Suit Figure B.1 and example of attacks Figure 4.14).

7.2.2 Design process to create Pedagogical Model to Design Serious Cyber Games

To create the new pedagogical design model we went through the following design stages, and this process was iterative and is linked to six steps in the CLE (Jonassen and Rohrer-Murphy, 1999).

Design Stage 1: List design model components.
Create a list of all the design decisions or fundamental theories, for example, from the final list created: Game Mechanics; Different Game Scenarios; Learning Hierarchy; Accountability Versus

Responsibility; Constructivism; Gamification; Self-Determination Theory; Threat Modelling; Security Threats; Security Defences; Design and Graphics; Role of Games Master; Role Play as Attacker; Role Play as Defender; Opportunity to discuss gameplay; Players' current knowledge; Related to Players' Role; and Real-World Problems (CLE steps one and two).

Design Stage 2: Sort and categorise design model components.
Sort items from design stage 2 into logical groups (CLE step three). Link back to activity theory see Figure 7.1. MOTENS example:

- **Multiple Modes of Learning:** D1) Games Mechanics.
- **Ownership Self-Learning:** D2) Different Game Scenarios.
- **Theory:** T1) Learning Hierarchy; T2) Accountability versus Responsibility; T3) Constructivism; T4) Gamification; and T5) Self-Determination Theory.
- **Environment:** D3) Threat Modelling; D4) Security Threats; D5) Security Defences; and D6) Design and Graphics.
- **Negotiation:** D7) Role of Games Master; D8) Role Play as Attacker; D9) Role Play as defender; and D10) Opportunity to Discuss Game Play.
- **Self-Learning:** D11) Players Current Knowledge; D12) Related to Players Role; and D13) Real World Problems.

Design Stage 3: Review for gaps in model.
Review list using current design models and gaps identified, either continue to design stage 4 or go back through from design stage 1.

Design Stage 4: Define high-level design model.
Develop the high-level model and detail model. This is an iterative process of logically grouping the design components in the detailed model back to the high-level model. In the creation of MOTENS, this took several iterations going back to change the categories in the high-level model, see Figure 7.3 and then re-defining the detailed model in Figure 7.6 before moving to the next design stage 5.

Design Stage 5: Develop detailed design process.
Develop the process and stages to go through to use the model created in stage 4 (CLE steps four and five). These are the detailed design stages starting from target players' segmentation through the selection of game mechanics' to meet target learning outcomes. Then the testing and evaluation stage (see example MOTENS five design stages subsection 7.3.1):

Stage 1 Segmentation of your target players.

Stage 2 What game do you want to create?

Stage 3 Create an initial MOTENS Design/Mechanics map based on target players segmentation.

Stage 4 Detailed steps to design the game.

Step 1 is the initial design decisions. **Step 2** decide the pre-game process. **Step 3** design gameplay. **Step 4** design end of game process, and **Step 5** review and test gameplay.

Stage 5 Testing and Evaluation.

Design Stage 6: Test model by mapping to serious cyber game.
Use the model created in design stage 4 and process in design stage 5 to map the game (CLE step 5, see example Figure I.13). This maps the pedagogical model to the serious game using the gameplay. For example, in Riskio, "the player selects a card from the top of one of the six STRIDE suits". This is linked in MOTENS to D8) Role Play as Attacker and theory T5) Self-Determination Theory.

Design Stage 7: Review the model
Review model for any gaps or conflicts. Go back to design stage 1 and iterate until the model meets defined requirements (CLE step six).

After some changes from feedback from supervisors, the model was ready for the formal testing, for illustrative case study see Section 7.4 and comparative case study see Section 7.5. In Section 7.3 the MOTENS model created using this process is explained in detail.

7.3 MOTENS Model

The model was created using the process defined in Section 7.2 based on the gaps identified in the current games for pedagogical assessment of serious games for cyber security awareness and education and experience of lessons learnt from the creation of Riskio. The model was designed to assist design serious cyber games for education and awareness rather than other categories of serious games, for example, secure software development.

The MOTENS model comprises six high-level components (see Figure 7.3), with other sub-categories (see Figure 7.6). The model is designed for serious cyber games to teach cyber security awareness and education. The link back to the activity model main components: Subject, Instrument, Object, Division of labour, Community and Rules, see Figure 7.1 are shown in brackets.

- **Multiple Modes of Learning** - The game mechanics that provide opportunities to learn a wide range of attacks and defences with players from different backgrounds (Instrument, Object, Rules).

- **Ownership Self-Learning** - Using Bloom's taxonomy, creating an environment where the learners take accountability and responsibility for self-learning and Bloomś higher-order thinking skills (Subject)
- **Theory** - Using a constructivist theory to develop the game and based on risk methodology known to the players (Subject).
- **Environment** - Create gameplay for players in a game setting they understand an appropriate learning environment (Division of labour).
- **Negotiation** - Change the role from teacher to coaching, not lecturing, and from content delivery to problem-based learning (Division of labour).
- **Self-Learning** - To create self-learning by use of problem-based learning; learning hierarchy; and build on players current knowledge (Community).

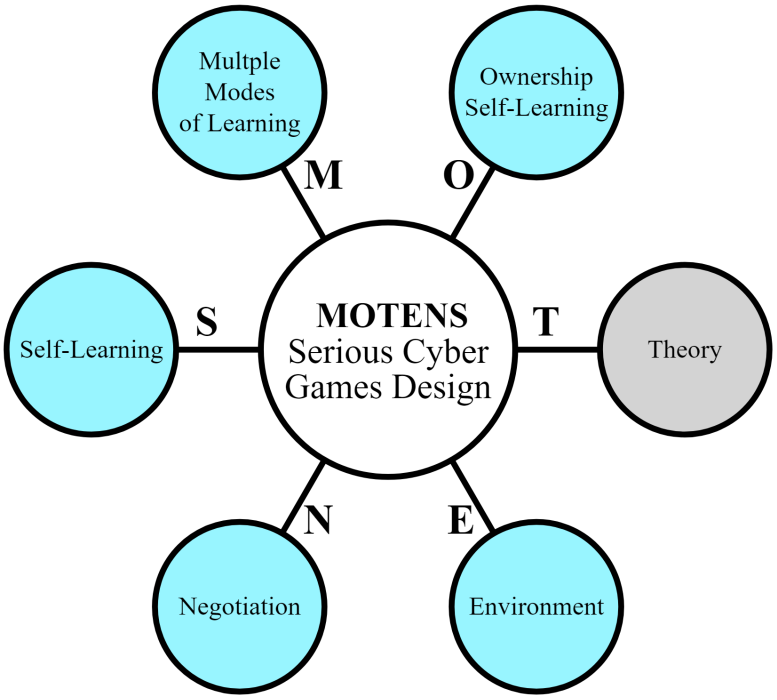


Figure 7.3: MOTENS Model.

Figure 7.6 shows the MOTENS model in more detail and will be used as the basis for a new model to design serious cyber security games.

7.3.1 MOTENS Design Stages

To design and create a serious cyber game, the proposed model takes you through the following design stages:

Stage 1: Target Game Players to identify and segment your target players into *non-gamers* and *gamers*. For example, Riskio primary target was employees, identified as non-gamers, with secondary group employees as gamers.

Stage 2: What game do you want to create, decide category either Secure Software development or Security Awareness and Education and then decide the types of serious game: Card Games, Computer Games; Board/Table Games; or Speciality Games. Decide if your game will have a games master. Figure 7.4 shows examples of serious cyber games by category and type.

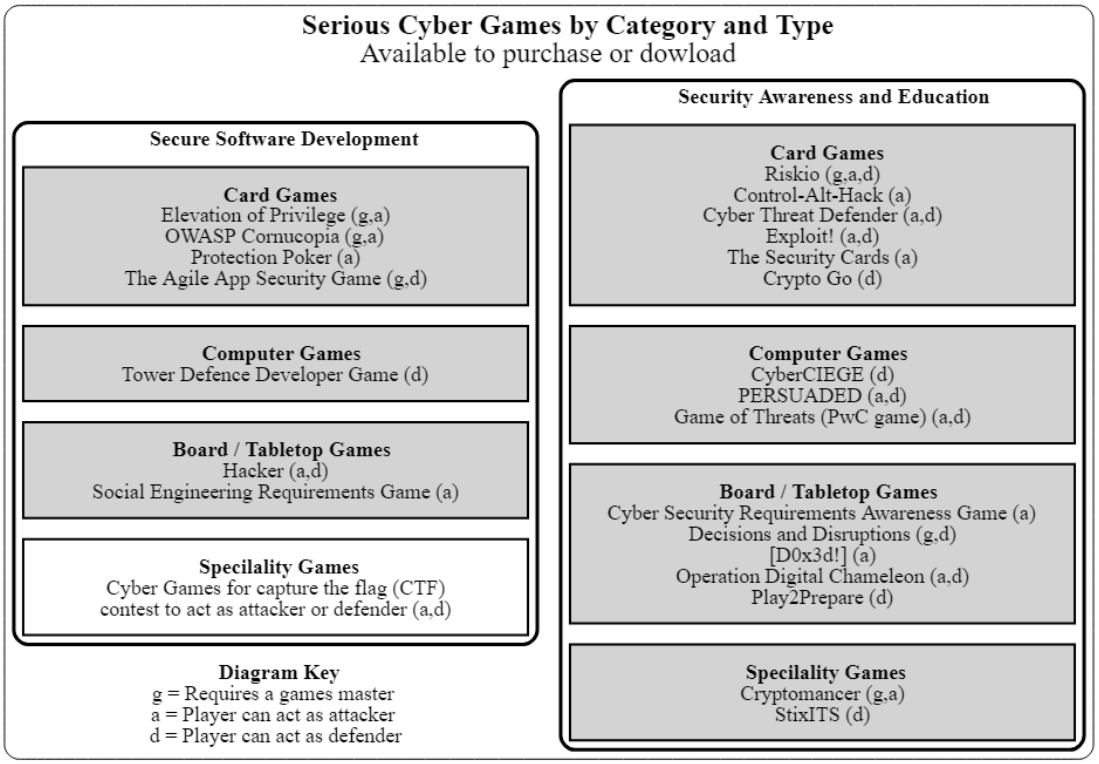


Figure 7.4: Serious Cyber Games by Categories and Type.

Stage 3: Create an initial MOTENS Design/Mechanics map. For example, it was noted that in mapping Riskio difference between Students and Employees with *D11) Players Current Knowledge*. Students' intrinsic motivation to accomplish and play the game was to want a high gamification level with a random selection of the attack card category. In contrast, employees wanted to learn and low gamification and select the attack category.

Stage 4: Design the Game, create the game using the MOTENS model. Go through five steps to design the game: Step 1 is the initial design decisions. Step 2 decide the pre-game process. Step 3 design gameplay. Step 4 design end of game process, and Step 5 review and test gameplay. Brief examples using Riskio: Step 1 Use Microsoft STRIDE for threat model and the defence cards NIST (NIST, 2021a) and NCSC (NCSE, 2020) frameworks. Step 2 before playing Riskio tutorial on Microsoft STRIDE for all players. Step 3 identified different requirements to allow employees to select the attack card category. Step 4 allow time for players to discuss the game at the end of

each round. Step 5 players had difficulty holding all cards, changed the design to print attack category on the back of the card and only select one card at a time.

Stage 5: Test and Evaluate by testing the game by playing with target players and changing design/mechanics if required from player feedback. In the example of Riskio, we used the TAM Model, see Figure 7.5.

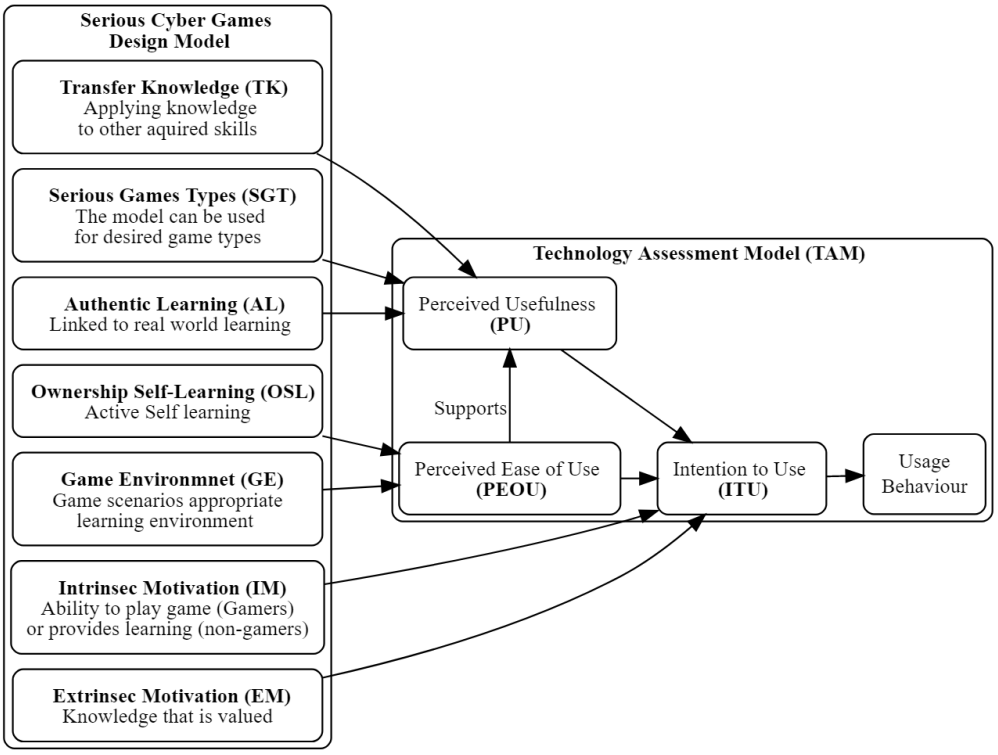


Figure 7.5: TAM Model linked to MOTENS Model.

7.3.2 Pedagogical Principles - MOTENS Model (Theory)

This section explains the pedagogical principles of the MOTENS Model. It is acknowledged that serious cyber games can provide an environment that motivates players to learn. However, an entertaining and fun serious game does not necessarily mean playing the game meets the game's objectives (Rooney, 2012). For this reason, the pedagogical model must integrate the gameplay supported by theory to ensure the game learning objectives are met. This section explains using the Riskio game how the MOTENS Model supports both the serious game design and how this is supported by pedagogical learning theory.

T1) Learning Hierarchy. Learners will sometimes memorise information without understanding the concept. For example, they may recite a Distributed Denial-of-Service (DDoS) but not comprehend its meaning. Reciting from memory would be an example of Bloom's taxonomy of lower-level thinking (Bloom et al., 1956). Gagné has proposed a *'learning hierarchy a set of component skills that must be learned before the complex skill can be learned'* (Gagné and

Briggs, 1992). Using the DDoS example, learners understand the issues around the 'availability' of systems, understand what a distributed attack is, and understand what a denial of service attack is. Learning these three components should join together to understand a DDoS attack and example in Bloom's taxonomy of higher-order thinking skills.

T2) Accountability Versus Responsibility. In serious games, accountability is the opposite of responsibility (Mayer et al., 2014). For players to be accountable, they must know the reason for playing the game and the effects or consequences. In contrast, responsibility is to critically reflect on the short and long-term value and consequences for playing. (McGonigal, 2011). Moreover, this is important in getting the players thinking from Bloom's lower-order thinking skills of retention through higher-order skills of understanding, applying, and evaluating to creating. For accountability, the games' rules and learning objectives must be clear to the players, and the players must value the learning objectives for responsibility.

T3) Constructivism. Constructivist learning theory states that the learning process is unique to the learner. Gamification theory looks at the learning process, which is from two different points of view at the same time. The first view uses an individual perspective, and the second view is from community-based learning (Bíró, 2014). Any instruction theory needs to include: methods of instruction, learning objectives, and conditions for instruction (Driscoll, 2000) and considers both these perspectives.

Methods of Instruction. The constructivism theory believes that learning occurs as learners are actively involved in meaning and knowledge construction instead of passively receiving information (Fosnot and Perry, 1996). The constructivist-oriented approach concentrates on the learners constructing their understanding during social interactions (Maor, 1999a). Therefore, gamification to teach cyber security awareness and education must promote the interactions that increase the discourse and personal construction. In the design of the Riskio game, we followed the principles of constructivism (Hart et al., 2020), which has been the predominant learning theory used in education programs for young children, college and university students (Fosnot and Perry, 1996; Rolloff, 2010).

In a constructivist learning environment, learners work primarily in groups, learning and knowledge are interactive, and facts and knowledge change with experience (Bada and Olusegun, 2015). There are a significant focus and emphasis on social and communication skills and collaboration and exchange of ideas. Social and communication skills are contrary to the traditional learning environments where learners work primarily alone. Learning is achieved through repetition. The subjects are strictly adhered to and guided by a textbook.

Driscoll (Driscoll, 2000) summarised the five conditions for instruction for constructivism are: (C1) complex and relevant learning environment; (C2) social negotiation; (C3) multiple perspectives and multiple modes of learning; (C4) ownership in learning; and (C5) self-awareness and knowledge construction, see Table 7.1 an example links between, constructivist five conditions, MOTENS Model and Riskio game mechanics.

Table 7.1: Constructivist Conditions linked to MOTENS with Riskio Example.

Constructivist Conditions	Link to MOTENS Model	Example in Riskio
C1: Complex and relevant learning	Environment: D5) Security Defences	Players using Riskio defence deck can learn complex and primary defences
C2: Social negotiation	Negotiation: D10) Opportunity to Discuss Gameplay	End of each round of attack and defence games master encourage players to discuss and learn from other players
C3: Multiple perspectives and multiple modes of learning	Multiple Modes of Learning: D1) Game Mechanics	Each Riskio game board can provide multiple metaphors and analogies and multiple interpretations, the hallmark of Cognitive Flexibility Theory (Spiro et al., 2003). In Riskio, you can change the perspective and mode with different case studies that support the game board
C4: Ownership in learning	Ownership Self-Learning: D2) Different Game Scenarios	Riskio can be played with different game scenarios, having contextualised game objectives, players are encouraged to self-learn, however, concern not all students achieve 'buy-in' (Perkins, 1991)
C5: Self-awareness and knowledge construction	Negotiation: D7) Role of Games Master	Games master helping players become aware of the thinking process, what theorists call metacognition (Driscoll, 2000)

Game Learning Objectives. The constructivist approach to identifying the learning goals emphasises the learning context. It is not to assure that students know particular things but rather to show them how to construct plausible interpretations (Duffy and Jonassen, 2013). The following objectives were identified for the pedagogical model using the constructivist approach for serious cyber games: *Transfer Knowledge (TK)* - Applying knowledge to other acquired skills; *Serious Games Types (SGT)* - The model can be used for desired game types; *Authentic Learning*

(AL) - Linked to real-world learning; *Ownership Self-Learning (OSL)* - Active Self-learning; *Game Environment (GE)* - Game scenarios appropriate learning environment; *Intrinsic Motivation (IM)* - Ability to play the games (Gamers) or provide learning (non-gamers); and *Extrinsic Motivation (EM)* - Knowledge that is valued.

Conditions of Instruction. It is proposed to use hypermedia designs, collaborative learning, problem Scaffolding, and problem-based learning to create constructivist conditions for instruction, examples of how implemented in the Riskio game. *Hypermedia Designs* uses game boards that are a small but complete subset of real-world environments; *Collaborative Learning* provides an opportunity for players to discuss at the end of each round the attack and various defences used. *Problem Scaffolding* interactions between the payers and the games master can provide different levels of support. *Problem Based Learning* case studies supporting games boards can state problems that players need to decide how to defend.

Link to Gagné Nine Instructional Events. The nine instructional events can be mapped to the MOTENS model, using Riskio gameplay as an example. 1) gaining attention, 2) Inform learners of objective: Tutorial at start of the game; 3) Stimulate recall of prior learning: Discussion at the end of each round and end of the game; 4) Presenting content: Using graphics and icons on game board understood by players; 5) Proving learning guidance: Using games board that are relevant to the players; 6) Eliciting performance: Players try to find most economical defence; 7) Proving feedback: Games master giving feedback on attacks and defence; 8) Assessing performance: and 9) Enhancing retention and transfer: Games master can act as an attacker using an information deck.

T4) Gamification. It is about applying game mechanics to non-gaming activities, for example, training to make the activity more engaging (Routledge, 2016; Deterding et al., 2011b). Serious games use these techniques to provide a fun, enjoyable educational environment where the game participants learn by playing the game. Gamification does not mean game design requires designers to concentrate on competitive features in the design between players. Studies have proven a positive influence of serious games using gamified cooperation to create meaningful connections amongst players, and it facilitates similar learning and motivational outcomes as gamified competition (Dindar et al., 2021). In MOTENS design, stage 3 (see Section 7.3) creates a design/mechanics map to consider selecting the game's correct game content to meet target players' requirements.

T5) Self-Determination Theory. Deci and Ryan (Deci and Ryan, 2008) proposed a macro-theory called Self-Determination Theory (SDT). Although the work started on SDT in the 1970s, it can be applied today to gamification. SDT presents motivation as extrinsic motivation, the external factors, and intrinsic motivation, the internal factors. SDT also presents three basic psychological needs: Competence - Can perform the activity well; Autonomy - Feeling you are in control; and Relatedness - Sense of belonging. You require all three basic psychological needs to be intrinsically motivated, and for extrinsic motivation, needs at least competence and relatedness must be satisfied (Conejo et al., 2019). Conejo & Hounsell (Conejo et al., 2019) propose

modifying the existing framework to assist designers of games. They suggest that some game design frameworks address motivation superficially, while others focus exclusively on motivation. Table 7.2 shows examples of links between SDT theory, MOTENS Model, see Figure 7.6 and the Riskio game.

Table 7.2: SDT linked to MOTENS with Riskio Game Example.

SDT Theory	Link to MOTENS Model	Example in Riskio
Competence	Multiple Modes or Learning: D11) Players Current Knowledge	Riskio game difficulty levels, enables all players to be able to find attacks and defences
Autonomy	Negotiation: D8) Role Play as Attacker; D9) Role Play as Defender	Players can select the category of attack and defence cards
Relatedness	Ownership Self-Learning: D2) Different Game Scenarios	Games boards can be changed to relate to players learning objectives

7.3.3 MOTENS Game Mechanics

This section explains the five components of the **MOTENS** Model linked to games design/mechanics.

D1) Game Mechanics. In stage 1 of the design, you segment the players into gamers and non-gamers and ensure that you select the correct level of gamified content for target players. For example, students (identified as gamers) might want the random selection of threat category by throwing a dice, whereas non-gamers will want to select threat category.

D2) Different Game Scenarios. You can select different game scenarios. For example, in Riskio (Hart et al., 2020), we used University Fees Office as this proved most popular with players' but could use network diagrams or other fictional settings.

D3) Threat Modelling. This is where you select a threat model. For example, in Riskio, we used Microsoft STRIDE as suited to our learning objectives. However still, you might want to use a different model. For example, a serious game about hardware supply chain uses CIST (Halak, 2021), a threat model created for the hardware supply chain.

D4) Security Threats. The game must expose the players to the most common threats. For example, for Riskio, we 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).

D5) Security Defences. The game defences should be based on a wide range of attacks and countermeasures. Published frameworks should be used to build on players knowledge, for example, NCSC Cyber Essentials (NCSE, 2020) and 10 Steps to Cyber Security (NCSC, 2021).

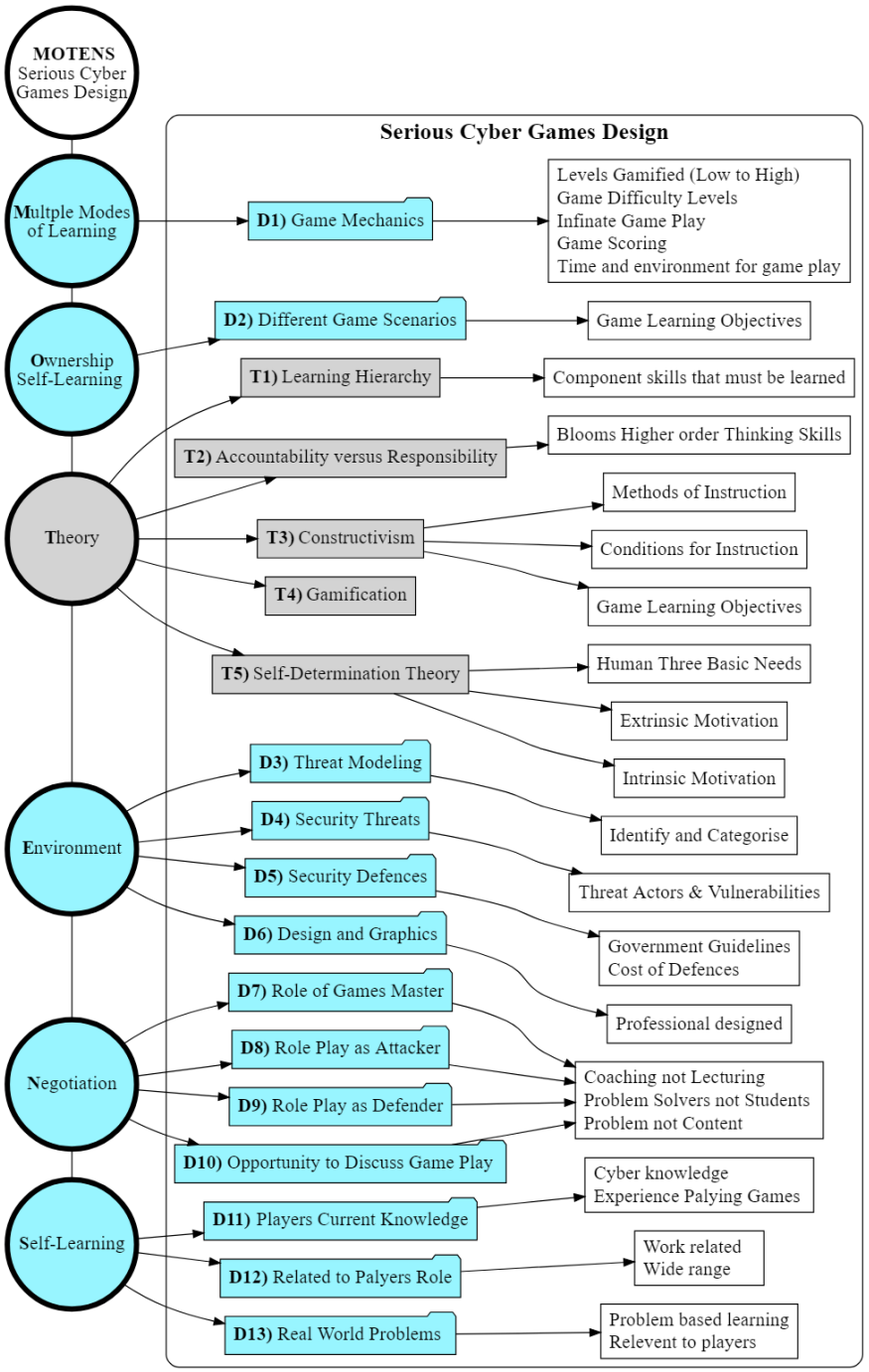


Figure 7.6: MOTENS Model Linked to Theory and Game Mechanics.

D6) Design and Graphics In design stage 4, you should test the game mechanics and gameplay and verify the design and graphics. For example, the quality of the design of logos, cards and icons can affect the players' enjoyment of the game, and this was noted in playing the early version of Riskio with home-printed cards. All graphics should be professionally designed, created, and high quality printed where required.

D7) Role of Games Master. If the game has a games master, their role is not to provide knowledge to the learners but to prompt and facilitate discussion. To enable prompt and facilitate

discussion can be done by designing stages in gameplay that facilitate discussion. The games master encourages learners' inquiry by asking thoughtful, open-ended questions and encouraging learners to ask each other questions. Seek elaboration of learners' initial responses; encourage learners to engage in dialogue, both with the games master and one another (C4: Ownership in learning, see Table 7.1).

D8) Role Play as Attacker. The design should convey the breadth of vulnerabilities and attack methodologies that attackers can exploit.

D9) Role Play as Defender. The design should improve the diversity of possible countermeasures that can be considered to prevent, detect, or mitigate cyber attacks. Players should learn the different defence strategies, and not all attacks can be prevented.

D10) Opportunity to discuss gameplay. The game should enable the players to cooperate and prompt and facilitate discussion about attacks and defences to create meaningful connections amongst players (Dindar et al., 2021).

D11) Players' current knowledge. The selection of some game mechanics can build on players' current knowledge. For example, if they already use a threat model consideration to use this in games design to build on players knowledge.

D12) Related to Players' Role. The designer can choose between creating a serious game where the player plays a work-related role or being given a specific role, such as the attacker.

D13) Real World Problems. The emphasis on solving should be on real-world problems (Seng Tan*, 2004) and move problem-based learning (Seng, 2000).

7.3.4 Assessment of MOTENS Model.

The next stage is to develop the MOTENS model into an illustrative case study and then test the case study with cyber professionals in higher education, researchers in cyber security and cyber professionals to test the model. The testing of perception will be for Perceived Ease of Use (PEOU); Perceived Usefulness (PU); Intention to Use (ITU); and efficacy of the new model, see Figure 7.5, which is based on the TAM model by (Yusoff, 2010). The TAM Model in Figure 7.5 maps serious games learning objectives to the TAM Model. Studies have revealed a lack of measuring the effectiveness of information security training (Nguyen and Pham, 2020). Many surveys ask questions focusing mainly on the knowledge and not the change in behaviour (Khan et al., 2011). The case study will be able to verify that the MOTENS Model has the potential to assist in the design of serious cyber games. However, there is still a lack of psychological theories to demonstrate increasing players' knowledge and changing security behaviours which is the ultimate objective of any security awareness and education training program. Using the MOTENS Model to design serious cyber games can link player motivations using SDT and use constructivism to link instruction, learning objectives, and conditions for instruction. The last

part in testing the game with players can link serious game objectives to the TAM Model to verify the perceived ease of use, perceived usefulness, and intention to use (see Figure 7.5).

7.4 Illustrative Case Study For Efficacy of MOTENS

This section sets out the illustrative case study used to evaluate the MOTENS model. The case study's goal was to demonstrate that the proposed framework effectively designs serious cyber games. The target audience for the case study is not users who would play serious cyber games rather people working in universities, research, PhD students and cyber educators. These are people involved in designing serious cyber games for awareness and education or conducting cyber security research.

7.4.1 MOTENS Illustrative Case Study Design

Assessment of Model. The next stage is to develop the MOTENS model into an illustrative case study and then test the case study with cyber professionals in higher education, researchers in cyber security and cyber professionals to test the model. The testing of perception will be for The design of the study based on the Technology Acceptance Model (TAM) that uses three constructs to predict the user acceptance of new technology (see Section 5.1). The participants were also asked three background questions and two questions on the level of expertise in cyber security technologies and cyber security awareness and education. We obtained ethical approval from the University of Southampton's Ethics and Research Governance Online (ERGO) system (Submission ID: 62140, see Appendix P).

The participants were emailed a link to a short video explaining the MOTENS model. They were given a case study (see Appendix I) explaining the background of the MOTENS model and using the Riskio serious cyber game (Hart et al., 2020) as an example of how the model can be applied to create a serious cyber game. The participants were then asked to complete a questionnaire with five background questions (see Table 7.3) and eight on their perceptions of the MOTENS serious games design model (see Table 7.4). See Appendix J for the complete questionnaire.

Table 7.3: Illustrative Case Study - Participant Background & Expertise Questionnaire.

Background	
Q1	Which team/function area do you work in at your organisation?
Q2	What is your knowledge of the Riskio game? (Tick all that apply)
Q3	What is your interest in serious cyber security games? (Tick all that apply)
Expertise	
Q4	How would you describe your level of expertise in cyber security technologies?
Q5	How would you describe your level of expertise in cyber security awareness and education?

7.4.2 Case Study Questionnaire

The questionnaire, see Table 7.4 was used to collect impressions about the proposed MOTENS pedagogical design model for serious cyber games. The results were aligned to 1 being a negative answer and 5 being a positive answer for the analysis. The hypothesis was formulated using the TAM model as follows to evaluate the MOTENS model:

- PU: The participants found the MOTENS model covered all types of serious cyber games and was useful (Q_1, Q_2).
- PEOU: The participants found that the MOTENS model would be easy to use and match the learning objectives to gameplay (Q_3, Q_4).
- PU: The participants agree on the value of using MOTENS to design serious cyber games to achieve desired learning outcomes (Q_5).
- PU: The participants agree on the value of using serious cyber games to achieve desired learning outcomes (Q6).

Table 7.4: Illustrative Case Study - Questionnaire MOTENS Serious Cyber Games Design Model.

Q	Category	Question
Serious Cyber Games Types (SGT)		
Q_1	PU	I found the model covered all types of serious cyber games I expected.
Q_2	PU	Using the I feel that the model would be useful in the design of the all the types of games: Card Games; Computer Games; Board Games; and Speciality Games (Education & awareness only for this type), see Figure I_5 in Case Study.
Games Environment (GE)		
Q_3	PEOU	I found the MOTENS model would be easy to use.
Q_4	PEOU	I found the MOTENS model was able to match learning objectives to serious games mechanics.
Authentic Learning (AL)		
Q_5	PU	I think using the MOTENS model to design serious cyber games will improve learning outcomes and give a greater chance to meet desired learning objectives of serious cyber games design.
Transfer Knowledge (TK)		
Q6	PU	I feel playing serious cyber games is an effective method to teach cyber security awareness and education and secure software development.
Intrinsic Motivation (IM) & Extrinsic Motivation (EM)		
Q_7	ITU	I would recommend the MOTENS model to anyone designing a serious cyber game.
Q8	ITU	Overall, I think the MOTENS model will be useful to design cyber games to meet intended objectives, and I would use it to help to design serious cyber games.

- ITU: The participants would use or recommend the use of MOTENS to design serious cyber games (Q7, Q8).

7.4.3 Threats to Validity

This section discusses the main threats to the validity of the MOTENS case study: construct, reliability, internal and external validity (Wohlin et al., 2012).

Construct validity. Construct validity aspect is to what extent the research aims and objectives represent what was in mind. The threat identified was anyone in the target participants who did not feel playing serious cyber games is an effective method and will negatively affect the MOTENS questions. The risk was mitigated by asking one generic question on the effectiveness of serious games to teach cyber security awareness and education.

Reliability. Reliability is the aspect concerned with the extent to which the data and the analysis are dependent on the specific researchers. The participants were required to have an overview of the MOTENS model before they answered the questionnaire. The identified risk is that the MOTENS presentation may vary in content and delivery even from the same presenter and affect the participants' questionnaire's answers. The risk was mitigated by recording the MOTENS presentation to ensure it was independent of the researcher presentation.

Internal validity. Internal validity is of concern when causal relations are examined whether one factor investigated is a risk that the investigated factor is also affected by a third factor. It was identified that participants who played the Riskio game used as an example in the MOTENS case study might be biased, and to mitigate against this, we asked a question about participants knowledge of the Riskio game, and so any possible bias could be analysed in the results.

External validity. External validity is concerned with the extent to which it is possible to generalise the findings beyond the case study settings. A potential threat could have been to select the wrong people to participate in the study. Although the questionnaire was anonymous, this was mitigated by asking a background question and excluding any questionnaires that did not meet the target audience.

7.4.4 Analysis of Case Study

For the analysis, the results of the questions from Table 7.4 responses have been aligned from 1 the lowest participant perception (strongly disagree) to 5 the highest participant perception (strongly agree) and displayed in Figure 7.7 in a box-plot diagram. The outliers are plotted as individual points. The calculation for the outliers was based on IQR to set the minimum and maximum values to be considered, see Equation 7.1.

$$IQR = Q_3 - Q_1$$
$$Q_1 - 1.5 \quad IQR \qquad Q_3 + 1.5 \quad IQR \tag{7.1}$$

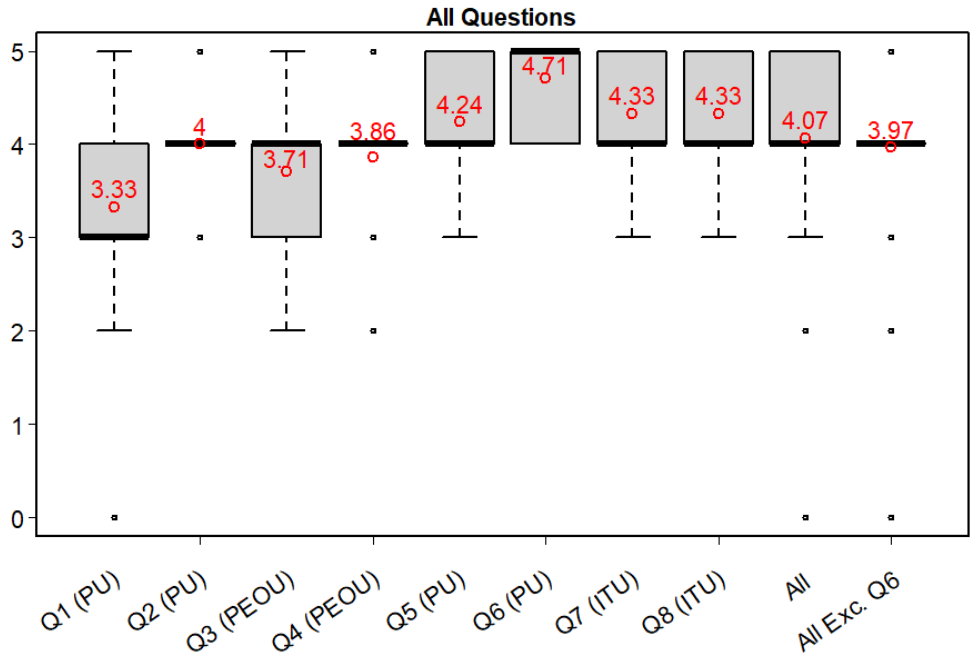


Figure 7.7: Illustrative Case Study - All Questions post review MOTENS Model (n=21).

Background Participants. The case study involved 21 respondents, 7 working as a university professor, associate professor or lecturer, 2 working in University Research Department, 5 PhD students, 1 MSc student and 6 from commercial organisations working in cyber awareness and education. Only 9 of the participants had read the Riskio published paper (Hart et al., 2020). The participants were asked two background questions to scale their expertise in cyber technologies and awareness and education. Both questions had similar means, expertise technologies 3.6 and expertise in education 3.2.

Threats to Validity. Question 6 was used to test the construct validity that participants have a general perception of the use of serious games with a mean score of 4.71. All respondents were scoring either 4 or 5 to indicate that all participants have a high perception of the benefits of using serious cyber games. Background question on knowledge of the Riskio game was used to test internal validity. The mean score of all eight questions in Figure 7.7 of the 9 participants with knowledge of the Riskio game mean score was 4.1, and the 12 respondents with no knowledge mean score of 4.0 and showed no significant difference. All the respondents met the required target for participation in the case study and had no identified risks to external validity.

Overall Perception. The results show the overall perception mean 4.07 (see Figure 7.8). There were some outliers, whereas, for example, one participant on question 1 on the MOTENS model covering all types of games commented, “I did not come into the exercise with an expectation”. The overall IQR for all 8 questions being between 4 and 5. Excluding question 6, which was the

generic question to test validity, the mean score was 4.71 and the same IQR between 4 and 5 (see Figure 7.7).

Perceived Ease of Use (PEOU). The mean score for questions 3 and 4 to test the PEOU was the lowest at 3.79. Question 3 regarding the MOTENS model would be easy to use had the broadest range of answers with an IQR between 3 and 4. Question 4 on MOTENS's ability to match learning objectives to game mechanics the participants having similar positive perception with a mean score of 3.86 with the IQR of 4. It can be concluded that participants can see how MOTENS can match learning objectives to serious games mechanics but feel it may not be easy to use.

Perceived Usefulness (PU). The MOTENS model mean score was 4.07, including generic question 6. The mean was 3.97 when excluding generic question 6. The IQR range was between 4 and 5. The participants' feedback was that they thought the MOTENS model could be helpful in the creation of serious cyber games.

Intention to Use (ITU). The overall mean score was 4.33, with all participants scoring either 4 or 5 for both questions 7 on a recommendation to use and question 8 helpful to meet intended objectives. Feedback from one external University proposed they would consider using the model for MSc students developing cyber games.

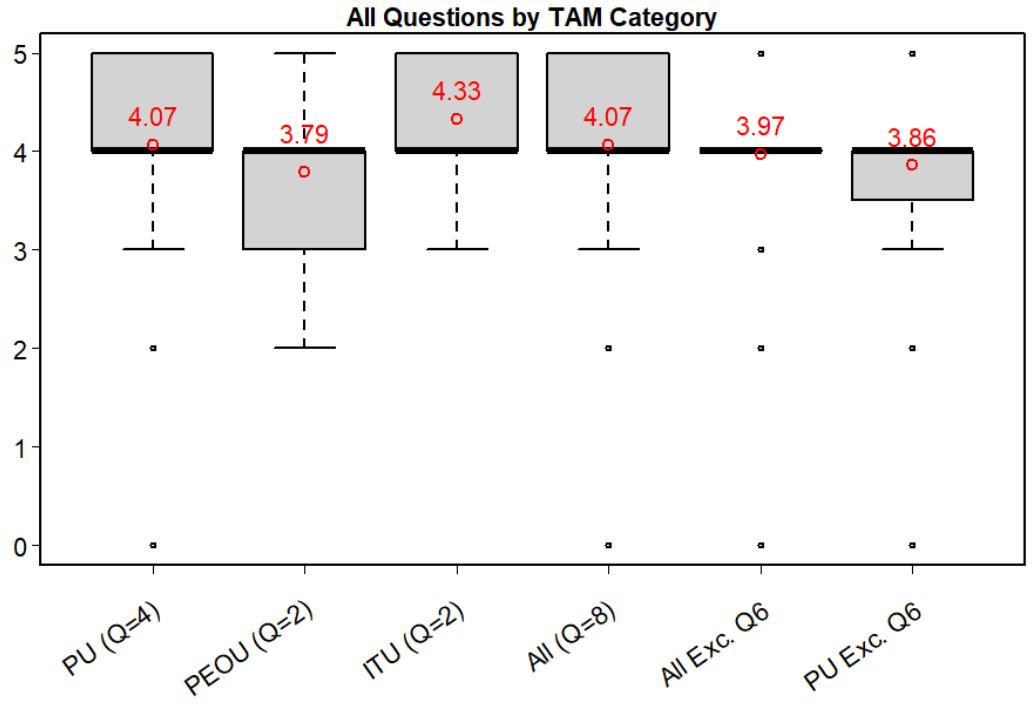


Figure 7.8: Illustrative Case Study - MOTENS Question 1 to 8 by TAM Category (n=21).

7.4.5 Conclusion Illustrative Case Study

The IQR for PU and ITU was 4 to 5. In contrast, IQR PEOU was 3 to 4 (see Figure 7.8). It was decided to create a second case study and target students who would use the model to design serious cyber games to test the PEOU in a comparative case study against another model.

7.5 MOTENS Comparison Case Study

This section uses a quasi-experimental comparison between the LM-GM and our new proposed MOTENS model. This study was to verify the MOTENS model ease of use by establishing the game mechanics' pedagogical intent in the model. This study targeted students who are currently designing serious cyber games or interested in designing serious cyber games.

7.5.1 MOTENS Comparison Study Design and Questionnaire

To evaluate the LM-GM against the MOTENS model, we used both models to map the Riskio gameplay. However, the LM-GM model has no concept of numbering notation. In the evaluation of Arnab et al. (2015), the participants used their numbering to map from the gameplay they identified back to the relevant model they were evaluating. The MOTENS model components are numbered, and to ensure validity, we added a notation to the LM-GM model for the comparison to MOTENS. The experiment involved an online presentation to MSc students on serious game design models of the LM-GM and MOTENS model using the Riskio game to apply the model principles and other presentations. The participants were then given an extract of Riskio gameplay applied to both models and given a questionnaire to score each model. As with the illustrative study in subsection 7.4.1, we used the Technology Acceptance Model (TAM) to test the difference between the new MOTENS and the LM-GM model. Participants were asked three questions about each model (see Table 7.5). Q1: Perceived Usefulness (PU); Q2: Perceived Ease of Use (PEOU); and Q3: Intention to Use (ITU). The participants' scores were aligned 1 to 5, and this enabled us to compare with the illustrative case study for MOTENS in subsection 7.4.1.

Participants were given a three-page case study, see Appendix K. **Page 1** was the TAM questions (see Table 7.5) asked for each model, see Figure K.1. **Page 2** was the LM-GM Model mapped to Riskio Gameplay see Figure K.2. **Page 3** was MOTENS mapped to Riskio gameplay, see Figure K.3.

7.5.2 Analysis of Study

The results of the analysis of the three questions are shown in Figure 7.9 with 11 participants. The first comparison of TAM scores illustrative case study in subsection 7.4.1, and the second is the comparison between MOTENS and LM-GM model.

Table 7.5: Comparison Case Study - Questionnaire LM-GM versus MOTENS.

Q	Category	Question Asked for both LM-GM and MOTENS
Q1	PU	It will be useful to use the model to help designing serious cyber games that are effective for players to learn desired cyber educational objectives.
Q2	PEOU	Using the model to design serious cyber games, I can see it will be easy to map gameplay to the game mechanics and support the pedagogical educational theory and learning, not just to create a fun game to play.
Q3	ITU	Overall, I think the model will help design serious cyber games to meet intended learning objectives and educational effectiveness. I would use it or recommend using it to help design serious cyber games.

Comparison to MOTENS in the illustrative case study The first case study (see Figure 7.8) and this study showed comparable results by the TAM category. PU mean as 4.07 and 4.45, and both have IQR 4 to 5. However, the PU median is 4 on the illustrative study, compared to PU median 5 testing differences between models. PEOU had similar means of 3.79 and 4.09, with only a difference in IQR of 3 to 4 in the first study compared to IQR 4 in this study. ITU in both studies has the same IQR and similar means of 4.33 and 4.18. The overall perception in the illustrative study of MOTENS, excluding generic question 6 was a mean of 3.97 compared to the mean of 4.24 in this case study. The overall results of the comparative testing study showed similar results as the illustrative study.

Comparison of MOTENS and LM-GM Model The difference between the LM-GM and MOTENS models using the TAM constructs (see Figure 7.9) showed MOTENS scoring a consistently higher score than the LM-GM model. The IQR of LM-GM for PU and ITU is 2 to 4, whereas MOTENS PU and ITU have IQR of 4 to 5. The LM-GM PEOU IQR is 2.5 to 3.5, whereas MOTENS is 4. The overall perception of LM-GM has a mean of 3.15 with IQR of 2 to 4, compared to MOTENS means of 4.24 and IQR 4 to 5.

7.6 MOTENS Summary and Conclusion

This chapter proposes a new pedagogical model called MOTENS to design serious cyber games to address current pedagogical models' limitations in designing and creating serious cyber games. The participants in the illustrative case study confirmed the consensus on the benefits of the potential use of serious games for cyber awareness and education. In the creation of the MOTENS model identified three critical areas in which the MOTENS model has improved on current models: 1) they do not link game mechanics to the learning objectives; 2) high-level model and will not assist in the selection of game mechanics to achieve serious game objectives;

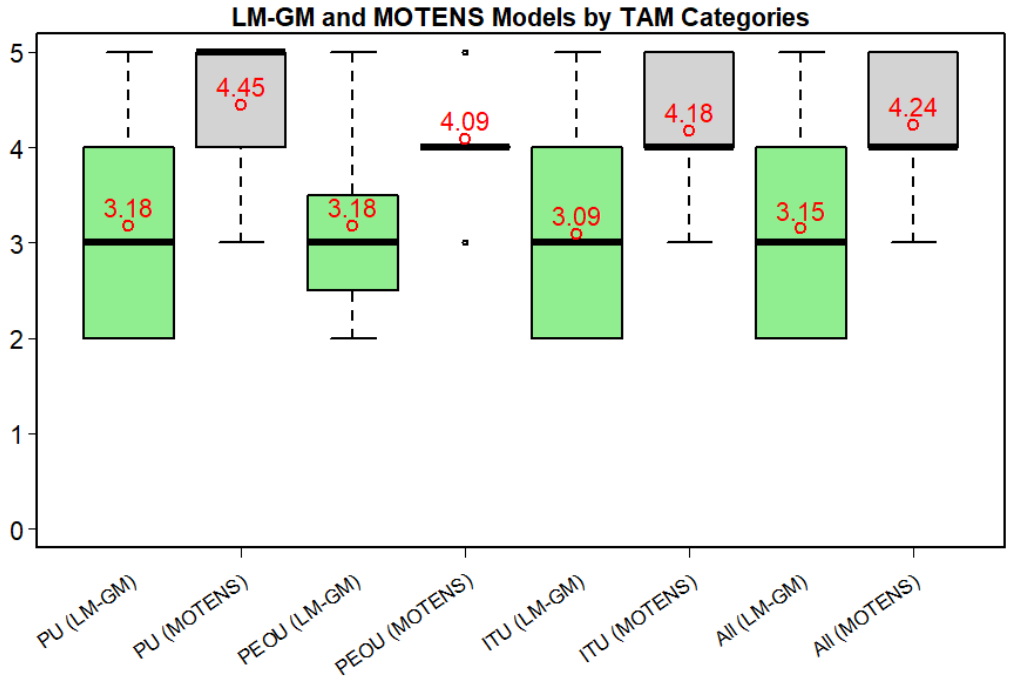


Figure 7.9: Comparison Case Study - MOTENS by TAM Category (n=11).

3) are mainly assessed in terms of the quality of their content, not in terms of their intention-based design. The improvements in these three areas using the MOTENS model are 1) Can link the game's mechanics to the target players and select the appropriate game's mechanics to meet the learning objectives, supported by pedagogical learning theory; 2) MOTENS has a five-step process to assist in the game design in stage 4; 3) Learning objectives are built into all six components of the MOTENS model and through the five stages in designing serious games. The case study showed that the participants using the Riskio serious game as an example of using the MOTENS model goes through the five design stages, which will assist you in selecting game mechanics. The case study example also shows the serious game design can be linked to pedagogical methodology, both the design of the serious game and how this is supported by pedagogical learning theory. Next, Chapter 8 explains how to use the MOTENS model to create a new serious game called CIST.

MOTENS was created to design serious cyber games, but it has the potential also to be used for existing games for assessment and improvements to the game design.

Part IV

Create New Game Using MOTENS a New Pedagogical Model

Chapter 8

CIST: A Serious Game for hardware supply chain

This chapter explains using the MOTENS model how to create a new serious game to educate players on the threats and possible countermeasures in the IC supply chain. The CIST game was created to show that you can create a different type of game and base the game on a different threat model using MOTENS, see Table 8.1 for crucial differences of a new game called CIST from Riskio game.

Table 8.1: Design for New Serious Game.

Description	Riskio	New Game
Threat Model	Based on STRIDE Threat Model	Based on CIST threat model
Type of game	Tabletop card game	Computer Game
Target Players	Employees & Students	Students Hardware Security
Games Master Required?	Yes	No
Multiplayer Game?	Yes	No

Section 8.1 explains the trend to outsourcing the IC supply chain. Section 8.2 issues with using current threat models for IC supply chain. Section 8.3 the CIST threat model used in the CIST game. Section 8.4 summarises the CIST game compared to Riskio, using the MOTENS design model and conclusions. Section 8.5, CIST game study design. Section 8.6, CIST game study realisation. Section 8.7, analysis and evaluation. Section 8.8, and finally the conclusion.

8.1 Outsourcing of IC Supply Chain

In the 1970s and 1980s, companies traditionally manufactured microelectronic devices that designed and produced integrated chips (Malli Mohan, 2010). In recent years, there has been a remarkable growth of outsourcing in the hardware supply chain and moved away from vertically integrated companies owned and operated manufacturing processes. The shift is most prominent at Apple while the company uses in-house design teams for iPhone, Apple TV, iWatch it then outsources chip manufacture (McKinsey, 2019). Fabless manufacturing is the design and sale of hardware devices and semiconductor chips whilst outsourcing fabrication to a foundry. Some companies may even outsource design teams for part of a complete IC design. This outsourcing has increased threats and serious challenges in new security attacks, particularly IC counterfeit and Hardware Trojan insertion (Halak, 2021). In 2016 it was estimated that electrical household appliances, electronic and telecommunications equipment were the most counterfeited types of goods, with an estimated value of GBP 2.5 billion of fakes imported in the UK (OECD, 2019). Counterfeited Integrated Circuit or Chip (IC) risks are not limited to financial loss to companies and the UK economy in lost tax revenues. They also pose a national security threat to critical services, such as healthcare and critical national infrastructure. Malicious state actors could use compromised counterfeit IC to gain information or used to sabotage critical services. Poor quality counterfeit IC could comprise health systems and cause loss of life.

8.2 Threat Models for IC Supply Chain

The globalisation and outsourcing of the IC supply chain have led to a more complex production cycle. Threat modelling can be used to identify the potential threats in the IC supply chain and possible countermeasures to detect or prevent. The current threat models have limitations, and for example, the Microsoft STRIDE model is used to categorise the identified threats in six categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege. STRIDE was designed to identify threats in software development. The DREAD threat method (Shostack, 2008; Singh and Singh, 2012) is used to characterise the risk associated with five categories of risks: Damage potential, Reproducibility, Exploitability, Affected Users, and Discoverability. Both of these models can be useful in risk analysis. However, they are not designed for hardware vulnerabilities in the IC supply chain. The threats used in these models can have different meanings, not applicable or missing threats (Di and Smith, 2007), see Table 8.2 summary STRIDE/DREAD applied to hardware vulnerabilities.

Other threats to hardware are missing in STRIDE and DREAD models, e.g. runtime threats and counterfeiting, which is different to spoofing. Spectre (Kocher et al., 2018) and Meltdown (Lipp et al., 2018) were discovered by independent groups of researchers and disclosed to Intel and other parties directly involved in June 2017. The vulnerabilities take advantage of program threads using simultaneous execution and use properties of memory allocation to gain access to a restricted area of memory segments. The feature that introduced this vulnerability was introduced

Table 8.2: STRIDE versus DREAD Threats to Hardware Comparison.

STRIDE Threat	**Comments**
Spoofing	Not applicable to hardware threats
Tampering	It can be applied to hardware
Repudiation	Not applicable to hardware threats
Information Disclosure	It can be applied to hardware
Denial of Service	It can be applied to hardware
Elevation of Privilege	Not applicable to hardware threats
DREAD Threat	**Comments**
Damage	It could be used to identify threats, but unless knowledge of how and context IC will be used can fully estimate damage
Reproducibility	It could be linked to the hardware threat of how difficult to complete the attack
Exploitability	Different meaning
Affected users	Different meaning – Counting potential number of users not relevant to hardware
Discoverability	Different meaning – Used in ranking threats

by Intel in the 1990s, over twenty years before this vulnerability was publicly known. The use of cloud services meant that one vulnerable virtual machine could allow a low-privilege process to access secret information such as passwords, cryptographic keys of files on other hosts on the same server by breaking isolation. This is evidence that a new threat model is required to try and find vulnerabilities and possible countermeasures when designing ICs or changes to the IC supply chain where using third parties.

8.3 CIST Threat Model

Historically engineers have relied on failures to learn and improve their designs (Moore et al., 2001). However, using threat models to understand the attacks can help engineers build stronger countermeasures and evaluate against different options to build better protection from attack (Bakhuys Roozeboom et al., 2017).

The CIST threat model (Halak, 2021) was designed for hardware security to overcome the different requirements for hardware threats and gaps in current generic security threat models identified in the introduction of this paper. The model covers hardware-related risks through the complete IC life cycle from design, manufacturing, a user using the IC within a system and recycling.

CIST aims to identify the threats to the IC supply in four categories: Counterfeiting, Information Leakage, Sabotage and Tampering. The threats for each category are:

- Counterfeiting: the aim of the attackers, in this case, is to imitate an original IC to produce a counterfeit fraudulently
- Information Leakage: the attacker aims to extract sensitive data from an IC at various stages of the IC life cycle
- Sabotage: the attacker aims to deliberately damage or destroy an electronic device such that it becomes lost, unavailable, or unusable
- Tampering: the attacker aims to undermine the integrity of a system and its ability to function as expected. Unlike sabotage, adversaries, in this case, do not want to affect the availability

8.4 CIST Game Conclusion

In Appendix M designed a new CIST game and used the MOTENS model to design the game following the five stages and in stage 4, the five steps of linking the selected game mechanics to supported cognitive theory in the MOTENS model. CIST was a different type of game to the Riskio Game and showed that it is possible to design a different type of game using the MOTENS model. See Table 8.3 for the design summary of both games, and the following sections, we evaluate the CIST game.

8.5 CIST Case Study Design

The CIST game for the study was based on thirty attacks (see Table 8.4), and each attack was linked to one CIST threat category. The attack may be possible by more than the adversary depending on the capability of the level of attack can complete. The attack may be possible in one or more locations (stages 1 to 6, see Figure M.10) in the IC supply chain, and last, there may be one or more possible defence from the attack, which can be different depending on the location. Each attack has a unique Attack ID and Sequence, see Figure M.19 as an example, Attack ID 15 and Sequence ID 28. The sequence ID was used to present the thirty attacks in a random order to the player.

Table 8.3: Example of design differences between Riskio Game versus CIST Game.

Design	CIST Game	Riskio Game
Stage 1: Target Players (Segmentation)	University Students with secondary group employees (employees working in the IC hardware supply chain)	University Students with secondary group employees
Stage 2: Type of Game	Hardware supply chain; Online game; Single-player; No Games Master	Fictional organisation; Tabletop game with cards and game board; Multi-player game; Requires Games Master
Stage 3: MOTENS Design Initial Map	Different requirements for D1) Game Mechanics and D4) Security Threats, See Figure M.1	Different requirements for D1) Game Mechanics, D2) Game Scenarios, D7) Role of Game Master, D11) Players Current Knowledge and D12) Related to Players Role; See Figure I.7
Stage 4: Design Gameplay/Mechanics		
Step 1: Game Design - Initial Decisions	Use CIST Threat Model	Use STRIDE Threat Model
Step 2: Pre-Gameplay	Online presentation	Presentation by the games master
Step 3: Gameplay	No time limit to player making choices	Games master gives time limit to answer/select cards
Step 4: Game End	Feedback on selected options	Feedback from the games master and players encouraged to discuss the game attacks and defences
Step 5: Review and Test Design	n/a	n/a
Stage 5: Design Test and Evaluate	n/a	n/a

Table 8.4: Case Study CIST Gameplay Questions

Attack ID	Seq. ID	CIST Category	Description of Attack
1	2	C	IC Overproduction – the adversary, can produce more copies by fraudulently imitating an original IC
2	1	I	Cyberattacks on IP companies (IP Piracy Attack), the attacker is trying to collect information

Continued on next page

Table 8.4 – continued from previous page

Attack ID	Seq. ID	CIST Category	Description of Attack
3	5	S	Rowhammer attack used as a mechanism by waging a persistent attack to cause a large number of errors
4	3	T	Fault Injection Attack - In this case, an adversary can induce errors during the computation of a cryptographic algorithm to generate faulty results
5	4	I	Chip reverse engineering attack – the attacker has access to a working chip file and is able to extract the IP gate-level Netlist using a range of tools and reverse engineering technologies
6	30	C	Selling defective chips Defective ICs are chips that have failed the functional or parametric tests or found to be out of spec, and subsequently placed in the market as authentic products
7	9	C	Recover discarded chips then repackaged and sold in the market as new
8	29	I	IP theft attack by a malicious engineer in the system on a chip (SoC) design house, who has access to third party IPs, can steal design secrets
9	20	S	Remote CLKSCREW (read as 'clock screw') attack that exploits the security of energy management systems in ICs to compromise the system's availability
10	27	I	Reverse engineering attack – by using De-capsulation that is the removal of the chip's packaging and De-processing, which consists of removing the chip layers one by one in reverse order and photographing each layer, this information will be used to re-construct the Netlist and ultimately expose design secrets
11	12	T	Hardware Trojan inserted by an attacker into the design file
12	7	S	An attacker can compromise the software updates or patch to add own functionality to gain control of a system
13	21	T	The attack is able to insert Trojan in the RTL code, during the system integration or during the manufacturing of the Integrated Circuit or Chip (IC)
14	8	C	An attacker has access to a fabrication facility and the ability to obtain a gate-level Netlist of the chip through reverse engineering or other IP piracy methods to clone the ICs

Continued on next page

Table 8.4 – continued from previous page

Attack ID	Seq. ID	CIST Category	Description of Attack
15	28	C	An attacker has access to fabricated chips and IC remarking tool to remark ICs
16	16	I	An attacker has Access to PUF response/challenge pairs and can complete a PUF modelling attack (PUF modelling attack)
17	13	S	An attacker uses a Rowhammer techniques to undermine the integrity of electronics systems by facilitating an elevation of privilege attack
18	26	T	The attacker is to be able to inject an intentional fault, using a series of techniques to manipulate the environmental conditions of a circuit, that results in the desired fault effect
19	6	I	An attacker installs a Trojan in an attempt to perform malicious operations (Side-channel analysis)
20	14	I	An attacker can break the isolation between different applications running on the same machine, which they can then steal/copy sensitive data from a victim process (Speculative execution attack)
21	25	I	An attacker uses microprobing by attaching a microscopic needle onto the internal wiring of a chip, which allows reading out internal signals and revealing sensitive data that are not meant to leave the chip
22	10	I	An attacker can compromise a cryptosystem by analysing the time taken to execute cryptographic algorithms (Cache timing attack)
23	19	I	An attacker can monitor the external outputs of the hardware while cryptographic operations are running with the goal of attempting to gain information which would result in the security of the device being compromised
24	17	C	An attacker can create copies of smartcard by monitoring the power consumption is able break the cryptographic functions create unauthorized signatures and clone the device
25	15	C	An attacker is able to recycle ICs and repackage them as new IC and able to pass physical inspection
26	24	C	A malicious foundry can replicate programmable data and overbuild the ICs because of transparency of their designed IP to the foundry that requires a complete description of the design components and layout to fabricate the ICs

Continued on next page

Table 8.4 – continued from previous page

Attack ID	Seq. ID	CIST Category	Description of Attack
27	18	C	A malicious recycling centres can recycle ICs as if they were new and can be used as ICs are not chip locked
28	11	I	An attacker has, collected a subset of all challenge–response pair (CRP) of the IC PUF and uses Machine Learning to derive a numerical model from this CRP data, which correctly predicts the PUFs responses to arbitrary challenges with high probability
29	23	I	An attacker in the untrusted foundry has access only to the complete IC design as by manufacturing the front-end-of-line (FEOL) layers and back-end-of-line (BEOL) in same foundry
30	22	S	An attacker can replace valid firmware images with malicious images or make alterations to existing firmware

The questions are scenario-based using the same methodology as the most globally recognised cyber professional certifications, for example, CISSP, CCSP and CISM. This is to stop people from using memory dumps and memorising the answers. They are usually long paragraphs with 3 or 4 questions. The design of the CIST questions is meant to be challenging and trying to get players to use Bloom's higher-order thinking skills of analysing, evaluating and creating (Bloom et al., 1956) and not memory skills. Example Attack ID: 12 - "An attacker can compromise the software updates or patch to add own functionality to gain control of a system". This example could be evaluated as a tampering attack. However, the motive seems to be to take control and, more likely, a sabotage attack. Whereas Attack ID: 13 - "Attack is able to insert Trojan in the RTL code, during the system integration or during the manufacturing of the Integrated Circuit or Chip (IC)". This is more likely to be a tampering attack.

Before conducting the study, the CIST game was evaluated by sending a link to an online game to PhD students cyber professionals. The attacks are all referenced by a unique ID for players to feedback questions to improve the game. We obtained ethical approval from the University of Southampton's Ethics and Research Governance Online (ERGO) system (Submission ID: 64746, see Appendix Q). The game is designed as a single-player game, and all players who won the game by gaining ten points were placed in a lottery for a small prize. However, the CIST game can be played in both gamified competition or cooperation. Social relatedness in gamified cooperation can be higher than in gamified competition (Dindar et al., 2021). Players were able to work individually or in teams. For testing, we were testing the process variables in how the game mechanics worked and the outcome variables to verify the learning objectives were achieved (Bakhuys Roozeboom et al., 2017). The design of the study was a self-assessment questionnaire based on the TAM, which will evaluate the game based on three constructs: 1) Perceived

Usefulness (PU), will the game be helpful to learn about threats and countermeasures in the IC supply chain, 2) Perceived Ease of Use (PEOU) is the game easy to use to meet the objectives, not just fun to play, and 3) Intention to Use (ITU) would the players recommend to play the game to learn about threats and countermeasures in the IC supply chain, see Appendix L for complete questionnaire.

For the nine post-game questions, see Table 8.5 to test the three TAM constructs. The PU questions, Q1, Q2 and Q3, were to test the CIST game learning features and Q4, Q5 and Q6 were to test learning outcomes. Q7 and Q8 were to test PEOU and final Q9 to test the ITU. The questions were scaled using a 5-point Likert scale, and in addition to this, the players were asked for anonymised feedback. Before the players played the game, they were given a brief tutorial on the CIST game, CIST threat model and most common threats to the IC supply chain.

Table 8.5: CIST Game Evaluation Post-task Questionnaire.

No.	Type	Question
	Section 1 – Perceived Relevance to IC Supply Chain (PU)	
		Learning Features
Q1	PU	Control - Players in control and can learn at their own pace
Q2	PU	Challenge – The game provides sufficient to challenge the players
Q3	PU	Feedback – Players know how to improve their answers through the game feedback
		Learning Outcomes
Q4	ITU	Threats – Players will be able to identify critical threats and locations in the IC supply chain
Q5	PU	Countermeasures – Players will be able to identify defence as a countermeasure to threats
Q6	PU	Autodidact – Players more likely to take control of self-learning over presenting the same 30 attacks in traditional classroom presentation
	Section 2 - Perceived Ease of Use (PEOU)	
Q7	PEOU	I feel that players would want to play this game to increase knowledge in risk management of the IC supply chain
Q8	PEOU	I feel playing the CIST game will be easy for the player to learn about a given attack about adversaries able to complete the attack and location and potential countermeasures
	Section 3 - Intention to Use (ITU)	
Q9	ITU	Overall, I would recommend using the CIST game to learn about hardware vulnerabilities in the IC. Supply chain and countermeasures

The same methodology for the data was used as with the Riskio case study (see Section 5.1), MOTENS illustrative case study (see Section 7.4), and MOTENS comparison case study Section 7.5) case studies, using Likert scale of 1 to 5 and boxplot diagrams used to show the outliers plotted as individual points. The calculation for the outliers was based on IQR to set the minimum and maximum values to be considered, see Equation 8.1.

$$IQR = Q_3 - Q_1$$
$$Q_1 - 1.5 \quad IQR \qquad Q_3 + 1.5 \quad IQR \tag{8.1}$$

8.6 CIST Study Realisation

The event was held on the University Campus on the 9th of July 2021 following Covid-19 guidelines and was advertised to relevant MSc/PhD students to register for attendance. The event was titled *'Workshop on Hardware Security Threats and Defence'*, and nineteen MSc/PhD registered for the workshop, which was voluntary. There were seven presentations in the morning session: 1. Primer on Hardware Security Risks; 2. Supply Chain Security; 3. Principles Unclonable Functions; 4. Principles of SAT-Hard Logic Locking; 5. Hardware Attacks on ML-based Systems; 6. Remapping-based Defences for Contention-based Cache Side-Channel Attacks and final presentation before lunch on the CIST game 7. Game Design for Hardware Security Education. Further presentation after lunch 8. Trust Computing Principles before the presentation of the CIST game.

Before the players played the CIST game, we briefly presented to summarise vulnerabilities and critical terms in the IC hardware supply chain. The game was demonstrated to show the game mechanics and examples of what to look for when reading the attack (see Figure 8.1). We told the players to pay particular emphasis on reading the attack as often it will be clear as to the CIST category of attack and the stage where this attack can occur. For example, we showed that in a 'Rowhammer attack', the attacker's motive could be to perform denial of service (Jang et al., 2017), a CIST sabotage category. An alternative motive could be an escalation of privilege attack (Xiao et al., 2016), a CIST tampering or an information leakage attack. The players were then given approx. Forty-five minutes to play the CIST game and during the gameplay were supported by the game's creator asking questions about individual attacks and getting feedback.

8.7 CIST Evaluation

A crucial part of the MOTENS model is in Stage 5: Test and Evaluate by testing the game by playing with target players and changing design/mechanics if required from player feedback. This section explains the evaluation of the case study to test the CIST game.

8.7.1 Player Background Questionnaire

Three background questions, Q1 to verify current role and two questions self-assessment of players. Q2 expertise threats to IC supply chain and Q3 expertise in hardware security awareness and education. A total of twelve players played the CIST game, six PhD students and six MSc

Figure 8.1: Presenting the CIST Game Tutorial to MSc/PhD Students before the Game was Played.

students (Background Question 1). They were asked to assess themselves on a score of 1 to 5. *Q2. How would you describe your level of expertise in threats to the IC supply chain?* and *Q3. How would you describe your level of expertise in hardware security awareness and education?*. In the workshop morning session of seven presentations, five of these are PhD students who also played the CIST game and are included in the evaluation statistics.

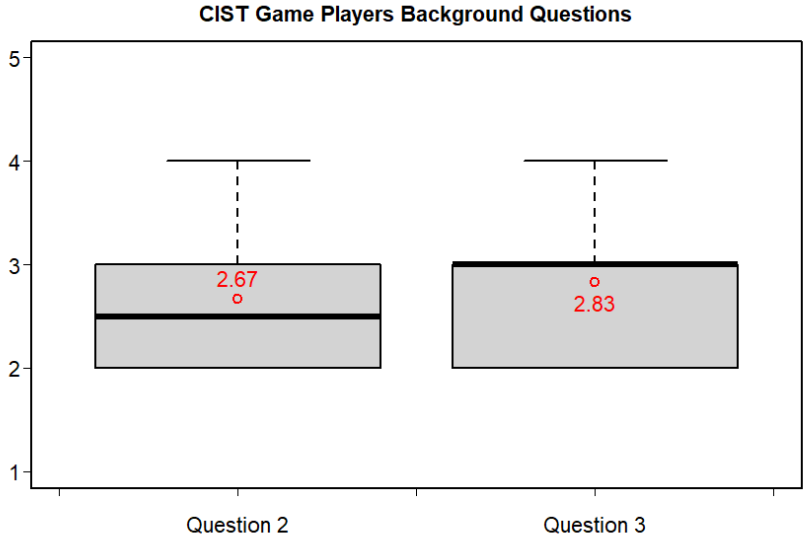


Figure 8.2: CIST Game Evaluation Q2. Expertise in threats to IC supply chain and Q3. Expertise in hardware security awareness and education (n=12).

The mean score for expertise in threats to the IC supply chain was 2.67. The mean score and a median of 2.5 for the level of expertise in hardware security awareness and education were 2.83 and a median of 3 (see Figure 8.2). These are very similar to the four Riskio experiments where

question 4 expertise in cyber security had a mean of 2.4, and median 2 and question 5 expertise cyber attack trends had a mean of 2.48 and median 2 (see Figure 5.2).

8.7.2 Feedback during Gameplay

The questions were designed for players to use Bloom's higher-order thinking skills (Bloom et al., 1956) however, players comment, *"if only we played this game after our lecture on vulnerabilities, we would have done better"*. The players used lower-order thinking skills and relied on memory recall (retention) instead of how they were instructed to read the attack for clues to the CIST category, location, and adversary. I went to each player more than once to walk them through an attack, and the following are examples of player feedback.

Example 8.1. *Attack ID 3: "Rowhammer attack used as a mechanism by waging a persistent attack to cause a large number of errors". Players could not see this was a sabotage CIST category, although the tutorial they were told rowhammer could be used as denial-of-service and escalation of privilege attack.*

Example 8.2. *Attack ID 7: "Recover discarded chips then repackaged and sold in the market as new". One player thought that because it says discarded that chips were faulty, they did not select the correct CIST category as counterfeiting.*

Example 8.3. *Attack ID 25: "An attacker is able to recycle ICs and repackage them as new IC and able to pass physical inspection". One player could not deduce from the question that this could only happen in Stage 6 Recycling IC. Another player could not deduce that there is only one valid defence. The list of possible defences, such as serial numbers, would not work as it says in the attack can pass physical inspection and requires 'x-ray inspection' as a valid defence to this attack.*

Example 8.4. *"Player complained that we should tell them where in attack cycle the attack is taking place, so they know which defence to select". This is a misconception as the player is referring to something like The Cyber Kill Chain® from Lockheed Martin[39]. It should be clear from the question what threat is, and they could decide where in the kill chain to stop the attack.*

When the players were walked through the attack and shown why the answers they generally agreed and then understood that they were not reading the attack clearly to get all the clues. On reflection, maybe we should have given more examples before they played the game in the tutorial presentation.

8.7.3 Post-task Questionnaire

There were nine post-task questions, six questions on PU (questions 1 to 6), two questions on PEOU (questions 7 to 8) and one question on ITU (question 9), see Table 8.5. Players could also

[39] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

leave comments, and nine out of 12 players left comments. The questionnaire was online and anonymous.

See Figure 8.3 for all nine questions. Question 1 about players in control who can learn at their own pace had the largest IQR between 3 and 5. Question 2 does the game provide a sufficient challenge for players with the smallest IQR of 4.5 to 5. The last question 2 also matches comments they found the game challenging (see comments on information in the game). Question 3 about player feedback had the lowest IQR and was also reflected in players comments. Questions 4 and 5 about threats and countermeasures had the same mean and IQR. Question 6 about 'autodidact' of players taking control of self-learning playing the game had a high IQR between 4 and 5 with a mean of 4.5 showing the value of serious games. Questions 7 and 8 about PEOU differed, where Q7 about risk management had a more comprehensive range of answers than Q8 about adversaries and countermeasures. However, both had similar means, Q7 4.5 and Q8 4.25. The last question 9 about ITU IQR 3.5 to 5 and mean 4.17.

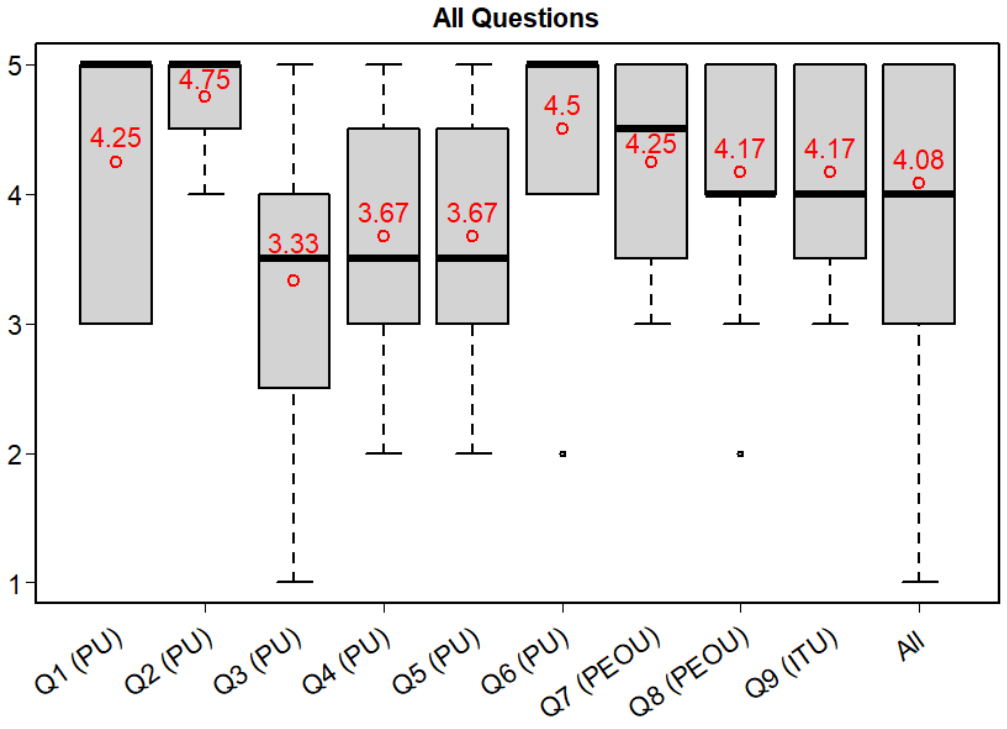


Figure 8.3: CIST Game Evaluation Post Game Questions 1 to 9 (n=12).

The nine comments can be grouped by two comments about game user experience and seven comments about information available in the game.

Comments on the user experience

> **Player 2:** "The user experience (UX) needs an improvement. The user interface (UI) is not straightforward, has not enough contrast, with not enough guidelines (these should be visual animations!), and a few unnecessary steps (e.g. the 'Get Answer' button)".
>
> **Player 9:** "It would be great if its more user friendly".

Comments on information in gameplay

Player 3: "If some paper link can be provided in the 'answer show', that would be great".

Player 5: "Explaining more details will be much better."

Player 6: "If this game can provide the reason why choose these countermeasures, I think it will be better."

Player 7: "It is a little bit difficult for beginners to play. Not familiar with the knowledge."

Player 8: "Can add explanations of those attacks and defences in result sections for players to learn. Instructions can be more clear, not easy to figure out how to play at first."

Player 11: "If some links of the paper of corresponding techniques are provided in 'answer show' would be good. Great game!."

Player 12: "Correct answers/suggestions could be better presented when wrong answer is given. Question wording could be clearer. For example, counterfeiting using stolen design files involves multiple steps, e.g. getting the design files, reproducing the design, preventing the knockoff being detected, detecting that the device is a knockoff. Mitigations could be in place at any of those stages: securing design files, making it fingerprintable (so copied design can be detected), procedures to check legitimacy of chip later in supply chain. It is not clear in the question which of these it means."

See Figure 8.4 for the nine questions by TAM category. All three TAM categories have the same median 4 and very similar means. PU of 4.03, PEOU of 4.21 and ITU 4.17.

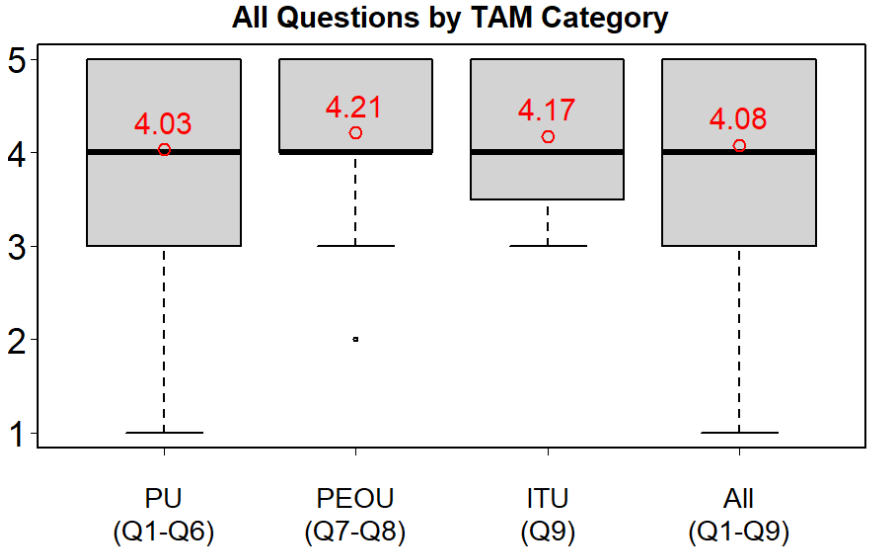


Figure 8.4: CIST Game Evaluation Post Game Questions by TAM Category (n=12).

Figure 8.5 summarises the six PU questions by questions 1 to 3 on learning features and questions 4 to 6 on learning outcomes. Both have the very same IQR between 3 to 5 and similar means of 4.11 and 3.94 are also similar medians of 4.5 and 4.

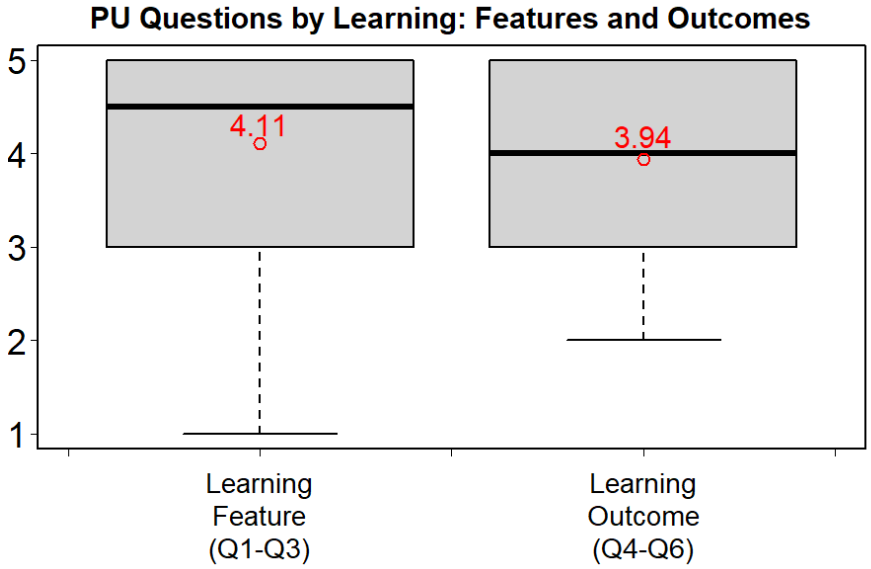


Figure 8.5: CIST Game Evaluation Post Game Leaning Questions 1-3 Features and Outcomes Questions 4-6 (n=12).

8.7.4 Using TAM Comparison between Riskio and CIST Game

We created the MOTENS pedagogical design model for serious games, from learning to creating and playing the Riskio game. The Riskio game is a tabletop multiplayer board game and played with a games master (see Chapter 4), whereas the CIST game is a single-player online game with no games master (Chapter 8). It is essential to compare the games' efficacy to verify that the MOTENS model can equally create different game types: card games, computer games, board/tabletop games and speciality games for security awareness and education, see Figure 7.4 cyber games by category.

Table 8.6 shows a comparison using TAM between Riskio (see Table 5.2) and CIST game (see Figure 8.4). Very similar mean scores for PEOU, PU and ITU. As with the Riskio game, the students had a wide range on the IQR for ITU of IQR 3 to 5 for students for Riskio and CIST students was IQR was 3.5 to 5.

8.8 CIST Game Summary and Conclusion

The CIST game was created to test the MOTENS model (see Chapter 7). The summary and conclusion here are using the evaluation of the CIST game to verify the suitability of the MOTENS model. The CIST game was designed to teach students about vulnerabilities and

Table 8.6: Compare using TAM Model Efficacy of Riskio Game versus CIST Game.

Description	Riskio Students	Riskio Employees	Riskio All	CIST Students
Numbers	**n=25**	**n=23**	**n=48**	**n=12**
Overall Perception Mean	3.59	4.26	3.91	4.08
PEOU Mean	4.2	4.39	4.29	4.21
PU Mean	3.48	4.27	3.86	4.03
ITU Mean	3.71	4.2	3.95	4.17
IQR for ITU & Median	IQR 3 to 5 Median 4	IQR 4 to 5 Median 4	IQR 3 to 5 Median 4	IQR 3.5 to 5 Median 4

defences in the hardware IC supply chain using the research aims and objectives. The critical question for this evaluation: "Did using the MOTENS model to design the CIST game create a game that could meet the learning objectives. Any failures noted in the game evaluation was it a result from design issues rather than a failure of a component or something missing in the MOTENS model?".

The following list gaps from feedback from the CIST game players and assessment if the gap is a failure of a design of CIST game or a failure in the MOTENS model failure.

Issue 1: Information in the game. Players 3, 5, 6, 7, 8, 11 and 12, all in the post-task questionnaire, gave feedback asking for more information on attacks, countermeasures and defences. A vital component of the MOTENS model is player feedback (D10 Opportunity to discuss Gameplay), and this is designed in several places. For example, Mark all attacks with a unique ID for players to give feedback (D10). After the player completed defence to the attack, feedback to the player if each answer on threat category, adversary, location and defence were correct. (D10). This issue would not seem a failure of the MOTENS model. We need to increase the information available to the players on additional information attacks and why the countermeasures are the correct choice.

Issue 2: User experience. Players 2 and 9, all in the post-task questionnaire, gave feedback about user experience. It is assumed that comments from player 2 are the same player when asked during gameplay. The player complained about clicking twice to get the answer and asked again gave no further feedback, and player 9 was a very generic comment on excellent if more user friendly. The feedback is related to the selection of defence as it takes one click to select the CIST attack category, four clicks to select adversary, and one-click to select the location of the attack. However, depending on the CIST category, the defence can take up to nine clicks to see all the possible defence options for the given attack. The alternative is to open a new page which would reduce the selection to two clicks. These comments do not seem to be linked to a failure in the MOTENS design model.

Issue 3: Identification CIST threat category. It was noted that players had difficulty in the identification of the CIST threat category. See examples 8.1, 8.2 and 8.3. We concluded that whilst the MSc/PhD students have experience eliciting defences to known attacks, they have no

experience in risk management and categorising threats using a threat model such as STRIDE or CIST threat models. The players lack of experience in categorizing threats would seem to be a mistake in gathering requirements in stage 3: MOTENS design initial map (see Figure M.1). We should have identified a difference in D11) Players Current Knowledge. The employees are more likely to have experience using threat models, and risk management is part of most organisations business as usual activities. However, the students would not be experienced in this. We could fix this by creating different game levels with more help for students and not a failure in the model itself.

Issue 4: Location of Attack in Kill Chain. Example 8.4, the player complained that we should tell them where in the attack cycle the attack is taking place, so they know which defence to select. We agree that we need to include the cyber kill chain in the tutorial before the game. It would also help explain the NIST five functions (NIST, 2021b) (see Figure 4.6). There may be more than one defence strategy, for example, 'protect', and the defence can target anywhere in the cyber kill chain.

Conclusions. None of the issues found evaluating the CIST game was identified as a failure in the MOTENS design model. As stated, "a vital part of the MOTENS model is in Stage 5: Test and Evaluate by testing the game by playing with target players". The changes to resolve all the issues found in stage 5, the "Design Test and Evaluate" of the MOTENS model, would be easy to change to resolve all the issues identified. The following Chapter 9 summarises the overall conclusions for the MOTENS model.

Part V

Conclusions, Contribution and Future Work

Chapter 9

Conclusions, Contribution & Future Work

In this chapter, we outline the conclusions (see Section 9.1), main contributions (see Section 9.2) of this thesis and present the future work (see Section 9.4).

9.1 Conclusions

This thesis proposes a new pedagogical model called MOTENS to design serious cyber games to address current pedagogical models' limitations in designing and creating serious cyber games. In the first MOTENS illustrative case study (see Section 7.4), the participants were people who would be involved in designing serious cyber games or working in research of cyber security. The results of evaluating the MOTENS scores were higher for Perceived Usefulness (PU), a mean of 4.07 median 4 and Intention to Use (ITU) mean of 4.33 and median 4, than the Perceived Ease of Use (PEOU) with a mean of 3.79 and where both PU and ITU IQR was 4-5, the PEOU IQR was 3-4 (see Figure 7.8).

The lower PEOU required a second study to test this again. The second case study (see Section 7.5) targeted students who would use design models to create serious cyber games using a comparative case study between the LM-GM model and the MOTENS model. The PEOU in the second case study improved with IQR of 3 to 4 for MOTENS in the first illustrative case study and to a IQR 4 in the second comparative case study with a mean of 4.09 and median of 4. Feedback from students who were designing serious games as part of their degree was very positive in early presentations of the MOTENS model and in the experiments (see Figure 9.1, extract of Figure 7.8 and Figure 7.9).

The two serious games designed using MOTENS model principles and following the design process has proved to be successful with target players see analysis of Riskio game study results Section 5.3 and CIST game Section 8.7. None of the issues found in evaluating the CIST game in

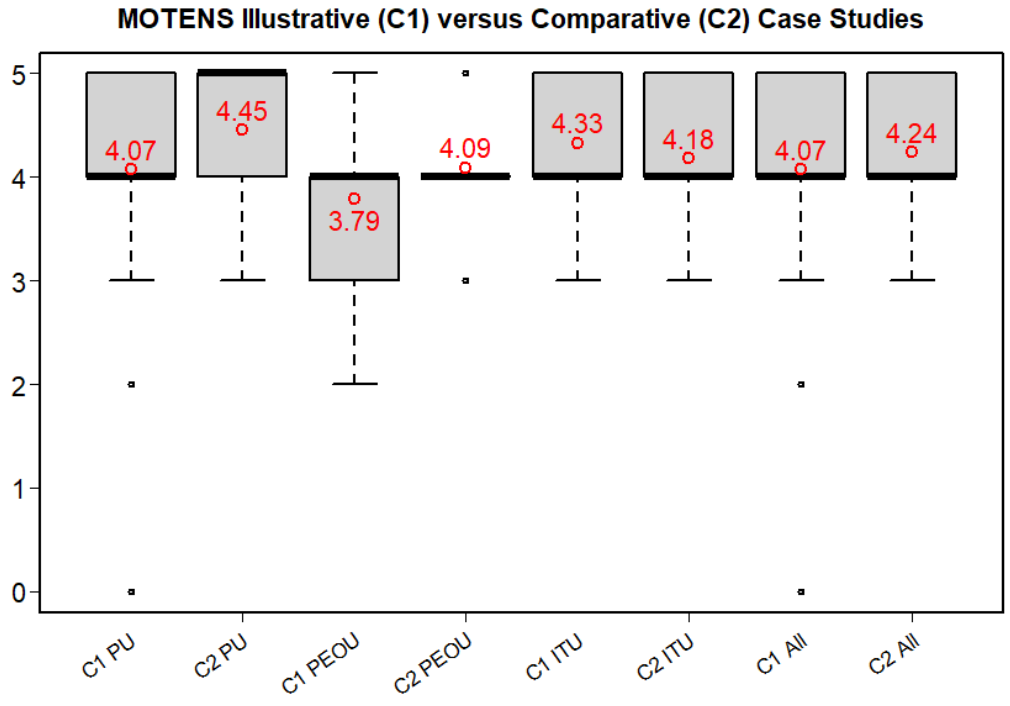


Figure 9.1: MOTENS Case Studies Evaluation by TAM Category (C1: n=21 & C2: n=11).

the last hardware security workshop experiment were identified as a failure in the MOTENS design model. The identified changes to resolve all the issues found can be linked to a required change in the game design and not a gap in the MOTENS model. Both Riskio and CIST games scored similar results with a difference in PEOU with a median of 5 for Riskio and 4 for CIST (see Figure 9.2, extract from Table 5.2 and Figure 8.4). We feel the difference was having the games master in the Riskio game but felt making the proposed changes identified in Section 8.8 CIST Game Summary and Conclusion will increase the CIST game PEOU score. It should be noted even excluding the more generic games questions from Riskio Q14-Q16, the results in Figure 9.2 are only fractional differences between the games.

Recalling the Research Aims and Objectives. This thesis adds a pedagogical model to design serious cyber games for awareness and education. The MOTENS model can create a wide range of different types of serious cyber games for awareness and education. Riskio, a tabletop card game, was used to create the MOTENS model from lessons learnt and designed for players from non-technical and technical backgrounds based on fictional university fees offices. However, you can change the game boards. The CIST game was created following the MOTENS model as an online game for technical students for risks in the hardware supply chain. The MOTENS model also allows adaption to use different threat models. The Riskio game-used threat model STRIDE and the CIST Game used Counterfeiting, Information Leakage, Sabotage, Tampering (CIST) threat model. Recalling the research aims and objectives, we have proved it is possible to create a serious cyber game using the pedagogical methodology using MOTENS for technical and non-technical staff. The games can be adapted to meet organisational and industry-specific threats

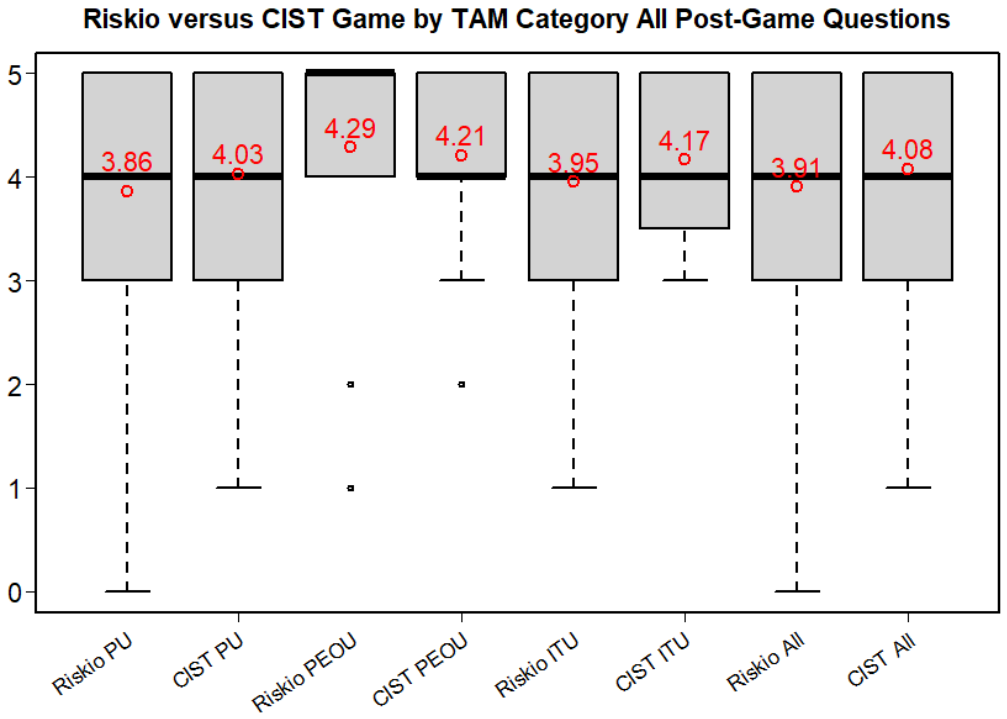


Figure 9.2: Riskio Game (n=48) (Students & Employees) versus CIST Game (n=12) by TAM Category.

and vulnerabilities by designing games that can change context exampled in Riskio game or specific industry risks game as evidenced in the CIST game.

Table 9.1 links the six research aims and objectives and how and where they are delivered in the MOTENS design model (see MOTENS design stages subsection 7.3.1).

Table 9.1: Research Aims & Objectives Linked to MOTENS Model.

No	Research Aim & Objective	MOTENS How Delivered
1	The model needs to be used to design serious cyber games for awareness and education. The games should not be restricted to any one type and can be card games, computer-based games, board/tabletop games or speciality games.	In Stage 2, the designer can select any type of game as the design model does not restrict which type. Riskio is a multi-player tabletop card game with game board and games master, whereas the CIST game is a single-player online game.
2	Must be able to design serious games for different target players, technical, non-technical and different backgrounds.	In Stage 1: Target Players (Segmentation), the players are segmented to assist in the design decisions.

Continued on next page

Table 9.1 – continued from previous page

No	Research Aim & Objective	MOTENS How Delivered
3	The serious games must be adaptable to create fictional contexts based on real-world problems.	The adaptability can be built into the design. An example of this is different game boards in the Riskio game an Office Diagram see Figure 4.9 and Network Diagram see Figure 4.10.
4	The design model must be adaptable to change the games designed to use different threat models.	In Stage 4, Step 1: Game Design can select the threat model used. In Stage 4, Step 2 can create different gameplay and test in Stage 5.
5	The model must be able to link the game mechanics to the pedagogical intent.	In Stage 3 designer creates an initial design map to find differences in target player groups, and Stage 5 selecting the game mechanics.
6	The model must be able to link industry standard defences as countermeasures to attacks.	In Stage 4, Step 1: Game Design - Initial Decisions: As evidenced in the design of Riskio and CIST games, the model allows the designer to select threat models, attacks and defences.

9.2 Main Contributions

The main contribution is MOTENS, a new pedagogical model to design serious cyber games for awareness and education. Also, two games were designed using the MOTENS design model. The first serious game called Riskio: A serious game for cyber security awareness and education, was designed as a multiplayer tabletop game. Riskio was designed and played to find, learn and test the critical design components that link the game mechanics to the cognitive theory of learning to create the MOTENS model. The second game, CIST: A serious game for hardware security supply chain, an online single-player game, was designed using the MOTENS model and used a case study similar to Riskio for the game evaluation.

In the creation of the MOTENS model, we identified three key areas in which the MOTENS model has improved on current models: 1) they do not link game mechanics to the learning objectives; 2) high-level model and will not assist in the selection of game mechanics to achieve serious game objectives; 3) are mainly assessed in terms of the quality of their content, not in terms of their intention-based design. We feel the improvements in these three areas using the MOTENS model in the current models available:

1) Can link the game's mechanics to the target players and select the appropriate game's mechanics to meet the learning objectives, supported by pedagogical learning theory.

2) MOTENS has a five-step process to assist in the game design in stage 4.

3) Learning objectives are built into all six components of the MOTENS model and through the five stages in designing serious games. The case study showed that the participants using the Riskio serious game as an example of using the MOTENS model goes through the five design stages, which will assist you in selecting game mechanics. The first detailed case study also showed how the serious game design could be linked to pedagogical methodology, both the design of the serious game and how this is supported by pedagogical learning theory. The second comparative case study, a comparison between the LM-GM and our new proposed MOTENS model, showed correlated results with similar means, median and IQR. However, we suspect that the simple addition of notation for the evaluation against MOTENS might have helped in the participants scoring the LM-GM model.

9.3 Lessons Learned

This section lists some of the key lessons learnt for future researchers into gamification for serious cyber games.

Literature Review. It is essential that if the research is over a long period that you continue to monitor for new papers in this research area, as can be seen in Figure 1.1, the increasing trend in the publication on gamification. It is recommended to complete bibliometric analysis and find top journals and leading scholars in gamification research and monitor for new publications.

Ethical Approval. Any experiments involving humans must have appropriate controls in place. Robson and McCartan (2016) also propose an increased emphasis on ethical issues, in line with greater awareness of the rights of research respondents (Goodenough and Waite, 2012). Data subject consent is more critical now as under UK Data Protection Act 2018 and GDPR, as data subjects have more rights than before over control of personal data. For example, the four experiments of the Riskio game were part of continued professional development (CPD). The players had a choice to participate in the research, and players were given a participant information sheet that clearly explained how their data would be processed (Appendix C) and also signed a consent form (see Appendix D).

Study Design. It is essential to use both qualitative and quantitative research for gamification. The motivation of the players can be found through quantitative data analysis using questionnaires. However, the opinions of the players' on the usage of the games can best be captured through qualitative data using observation of gameplay and interviews before and after the game (Hursen and Bas, 2019).

Game Testing. The graphic design, illustration, size and quality of paper printed on the cards significantly affect the players' enjoyment and motivation to play the game. You can use home-printed cards (see Figure 4.1), but as soon as possible should get cards and any physical game elements professionally printed or may cause a bias in players response to the game. This was observed from comments from academic team in playing with the home-printed cards in the base Riskio game (see subsection 4.1.1).

Games Master Experience. If the game requires a games master, as exampled with Riskio, the game master must give real-world examples. For example, encryption was not applied to laptops for the University Fees game board. The games master could provide an example in an attack where laptops were shared devices and organisations had roaming profiles. The CEO previously used the shared laptop, and all his files are cached on the laptop, which was left unattended in the fees office and stolen. Because of no encryption, the attacker has access to the CEO files cached on the laptop. The players preferred the real-world examples, and the games master must be an experienced cyber professional.

9.4 Future Work

The following areas have been identified for future work to continue to develop the MOTENS serious cyber games design model and develop Riskio and CIST games:

Publishing Riskio Game. Riskio has a website[40], and the game is for sale to universities, researchers and other interested organisations. The game is presented in a shallow gift box, 310 x 215 x 35 mm. The card decks are placed inside with A3 double-sided game board cut in half with the rules booklet, see Figure 9.3. The Covid-19 pandemic delayed the printing of the game. The game has been sent out to Universities and commercial organisations from Canada, Germany, India, Italy, Jersey, Switzerland, the UK and USA etc. Some of these requests are from organisations that use Riskio to train new graduates. One request from a significant USA federal government not-for-profit organisation and the game is already used for graduate intake for a national UK cyber research company.

Further Development of Riskio Game. The Riskio cards were designed using Adobe InDesign, and the plan is to make the cards available as editable PDFs for other researchers who can create their own question sets and game boards to change the game context as required.

New Game based on the CIST Game. The CIST game was designed for a specific target audience of university students on IT-related courses. The plan is to develop a new game for non-technical players and use the single-player online game based on a fictional organisation to teach NCSC Cyber Essentials (NCSE, 2020) and NCSE 10 Steps to Cyber Security (NCSC, 2021). The player can click on the tiles to select their defences based on NCSC defences with notional costs and effort to implement and maintain. Then the player chooses an attack and can

[40] www.riskio.co.uk

Figure 9.3: Riskio Game Board & Card Decks as Published Game.

Game Contains:

- Box for game 310 x 215 x 35 mm
- Rules Booklet
- Attack Deck 6 Suits
  - **S**poofing Suit
  - **T**ampering Suit
  - **R**epudiation Suit
  - **I**nformation Disclosure Suit
  - **D**enial of Service Suit
  - **E**levation of Privilege Suit
- Information Deck (for Games Master)
- 5 x Defence Decks (for Players)
- A3 Doubled-sided Game Board

find if they successfully defended the fictional organisation against the attack and how cost-effective their defence choices were.

Development of MOTENS Model. The case studies found that MOTENS could improve PEOU and further work on testing and improvements to the MOTENS model, including other games for cyber security awareness and education.

Serious Games for Secure Software Development. This thesis concentrated on designing serious cyber games for security awareness and education. However, as identified, an alternative is games for secure software development (see Figure 7.4), for example, the Microsoft Elevation of Privilege (EoP) game. The MOTENS model could be adapted to create a serious cyber game for secure software development. However, we hypothesise that the design of speciality games for secure software development like capture the flag serious games may require the pedagogical model to have additional design elements not needed for any other game types.

Pedagogical for designing serious cyber games versus evaluating serious cyber games. This thesis proposed the MOTENS model based on lessons learnt from creating the Riskio game and creating a new game called CIST. However, MOTENS could also be used to evaluate existing cyber serious games. A bias exists as the author of this thesis developed both games assessed. Several serious cyber games need to be tested to verify the MOTENS model suitability to assess serious cyber games. MOTENS use for evaluation may require changes over the use of MOTENS to design new serious cyber games.

Appendix A

Riskio Game University Fees Case Study

Background
The University Fees Office is responsible for processing fees and bursaries for the University to the approx. value of £180 million per year.

The University Fees office is open normal business hours Monday to Friday but also has facilities online for students, teaching staff and fees office staff to:

- Students - update personal and financial information and view financial transaction history, including update personal information; updating bank account details; and make online payments
- Teaching staff – view status of students' payments
- Fees Office Staff – can work remotely on students' records, including updating, deleting.

Staff
The University Fees Office has a team of 10 staff with the office manager and four staff on a rota working in the ground floor area. Staff have roaming profiles and can log into any PC/Laptop on campus. If they keep any documents on a personal drive, these will also be cached on any device they log into the network.

- John S is the Acting Office Manager and has worked for the University in several roles across the campus for ten years and in the last three years in the University Fees Office. He is currently acting up as office manager whilst the Office Manager is on long term sick leave.
- There are 4 reception staff work on a rota basis with no more than two people at the reception desk at any given time, but sometimes in quiet periods may only have one person

at the desk. When reception staff are not working on the ground floor upstairs working on other duties to do with University fees and bursaries.

Visitors
The students and teaching staff who visit the office have free movement in the public area and access a PC in the corner with internet access. The back-office area is strictly controlled by PIN and University issues ID card which acts as fob access to the door controlled security. However, the office manager does have visitors from students, university staff and outside visitors at his discretion.

Building & Security
The building is located on campus and has the following security features:

- Safe is alarmed and linked to 24x7 monitoring service – the safe holds limited cash but a large number of sensitive files, including credit/debit card information covered by PCI DSS
- Limited CCTV recording and last 5 days kept
- Front doors are locked and alarmed outside business hours
- Reception desk has a shutter that can be pulled down and locked
- PCs and Laptops are not encrypted, but require valid username and password to logon
- Office is cleaned out of hours by an outsourced cleaning company

Remote Access
Staff can access the services remotely through the website by using their University computer account username and password.

Appendix B

Riskio Card Decks

The Riskio Game has three card decks:

- Attack Deck
  - Spoofing Suit, see appendix B.1
  - Tampering Suit, see appendix B.2
  - Repudiation Suit, see appendix B.3
  - Information Disclosure, see appendix B.4
  - Denial of Service, see appendix B.5
  - Elevation of Privilege, see appendix B.6
- Defence Deck, set given to each player, see appendix B.7
- Information Deck, set for only Games Master, see appendix B.8

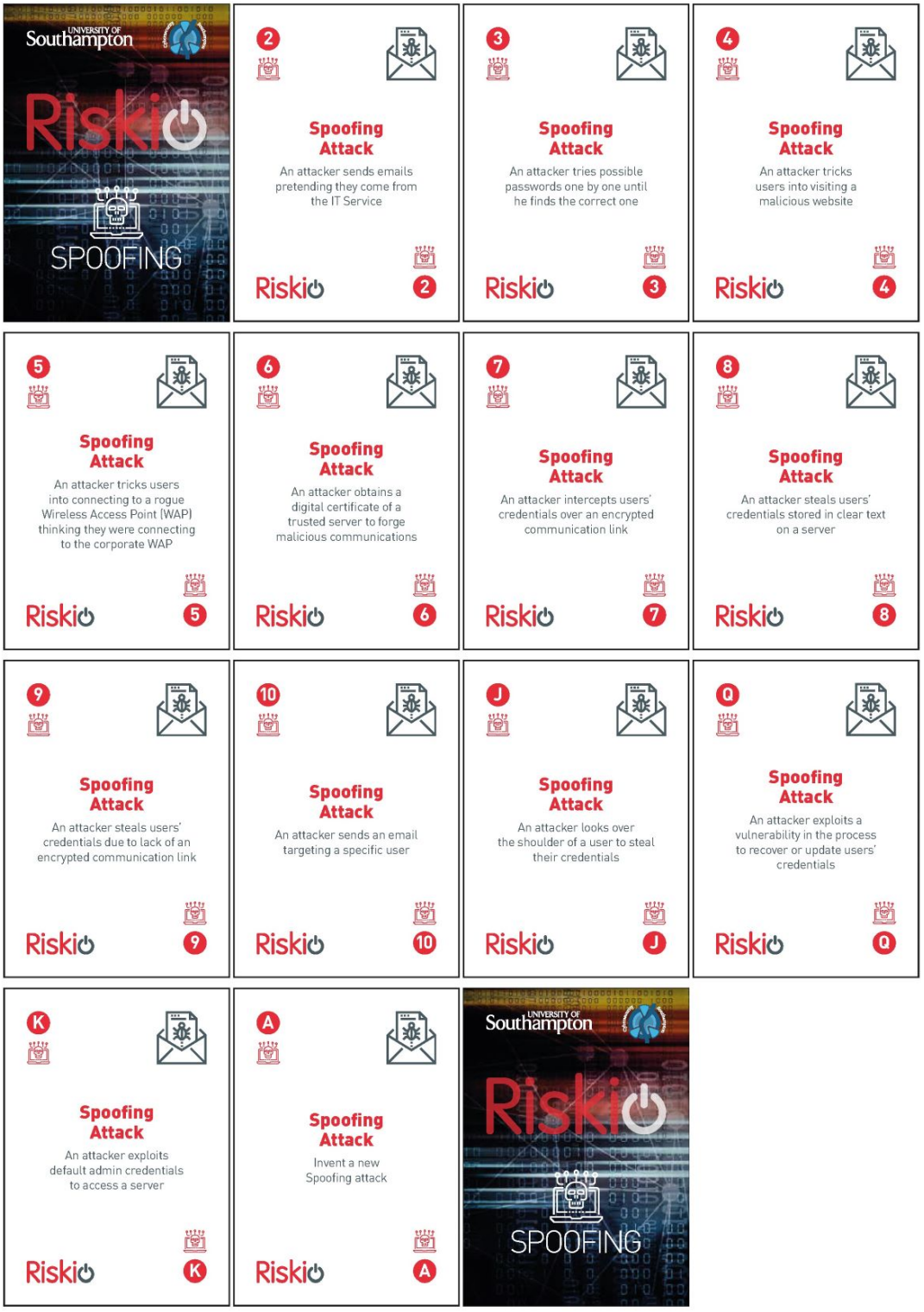


Figure B.1: Riskio Game Attack Deck - Spoofing Suit.

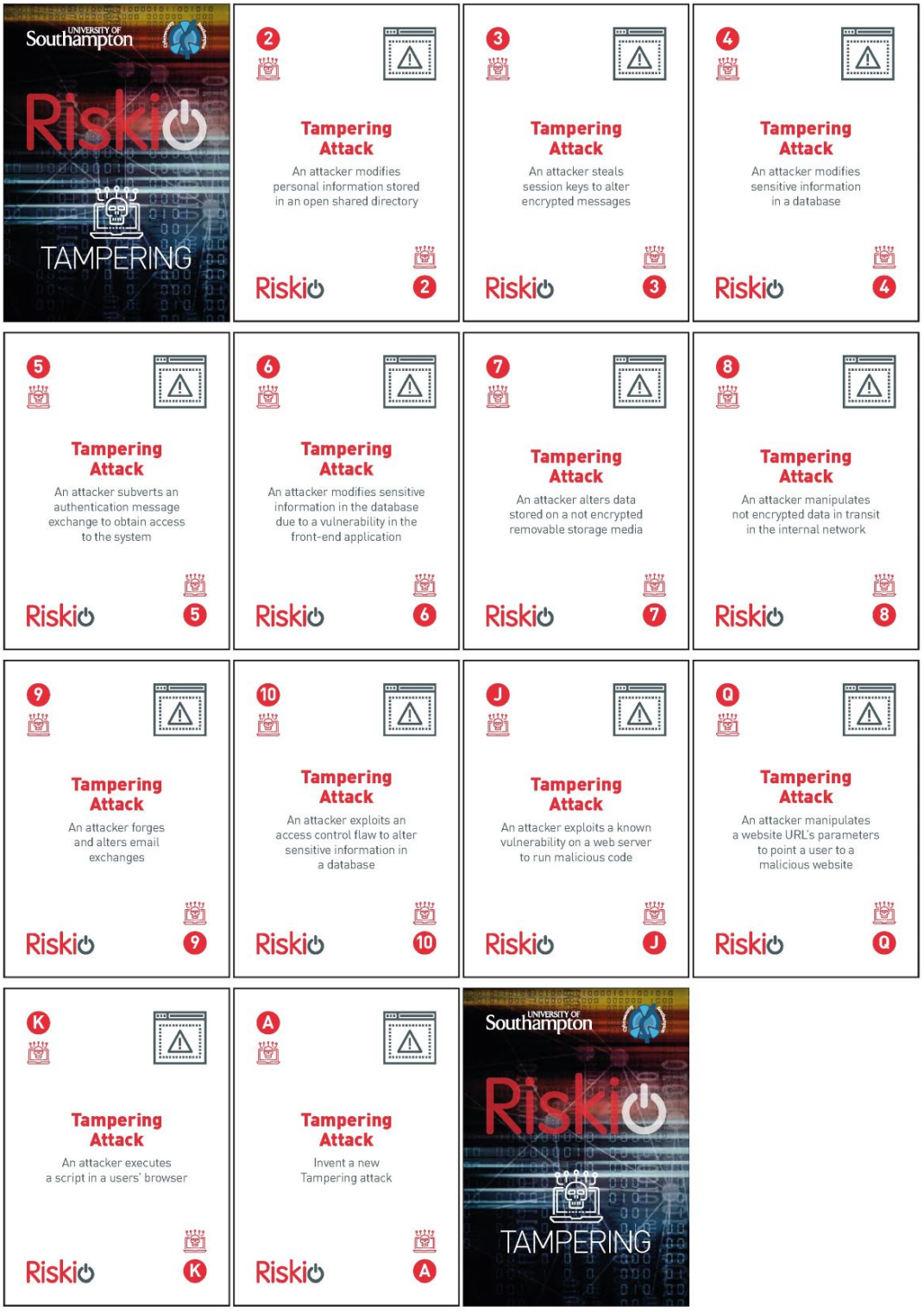


Figure B.2: Riskio Game Attack Deck - Tampering Suit.

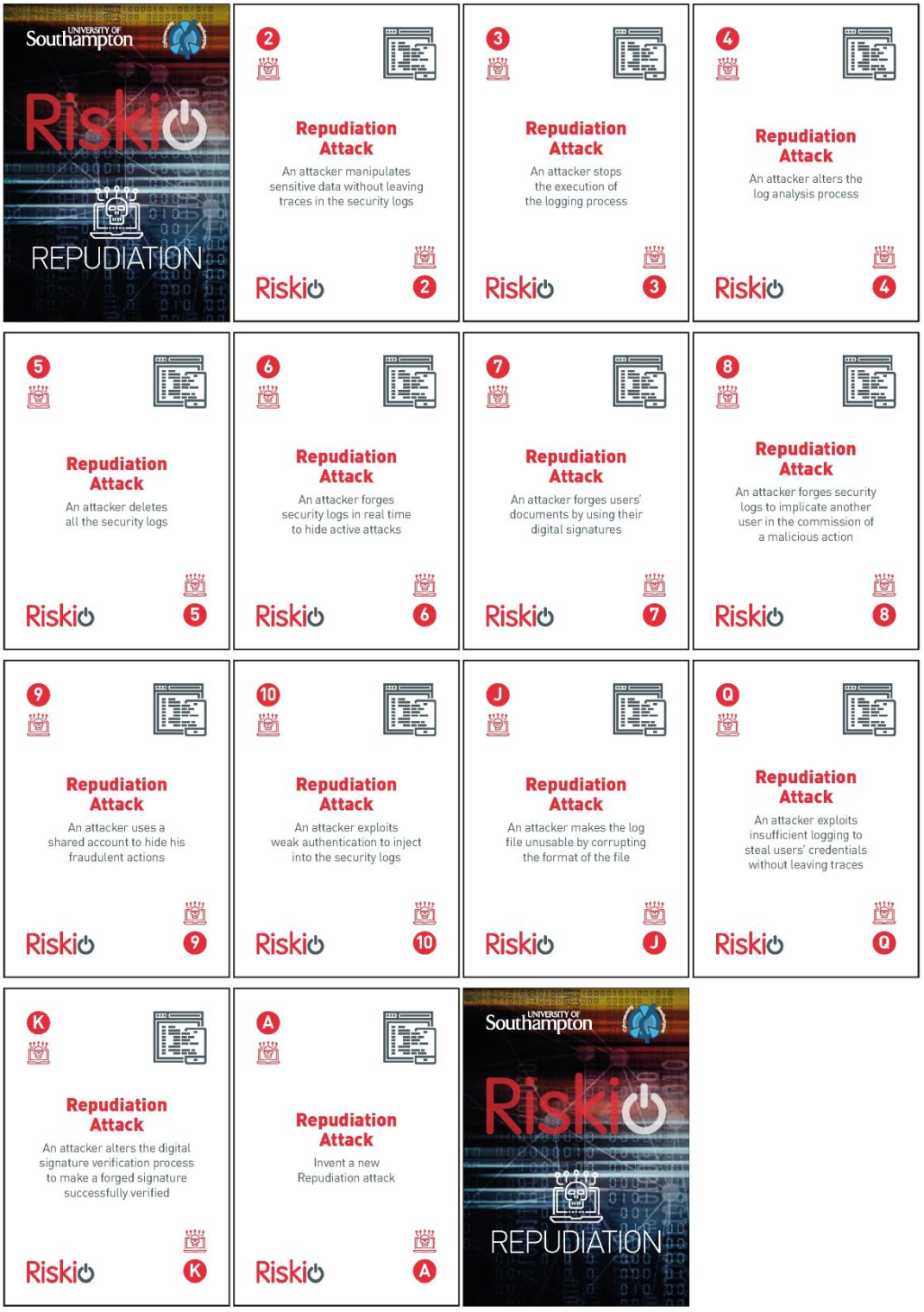


Figure B.3: Riskio Game Attack Deck - Repudiation Suit.

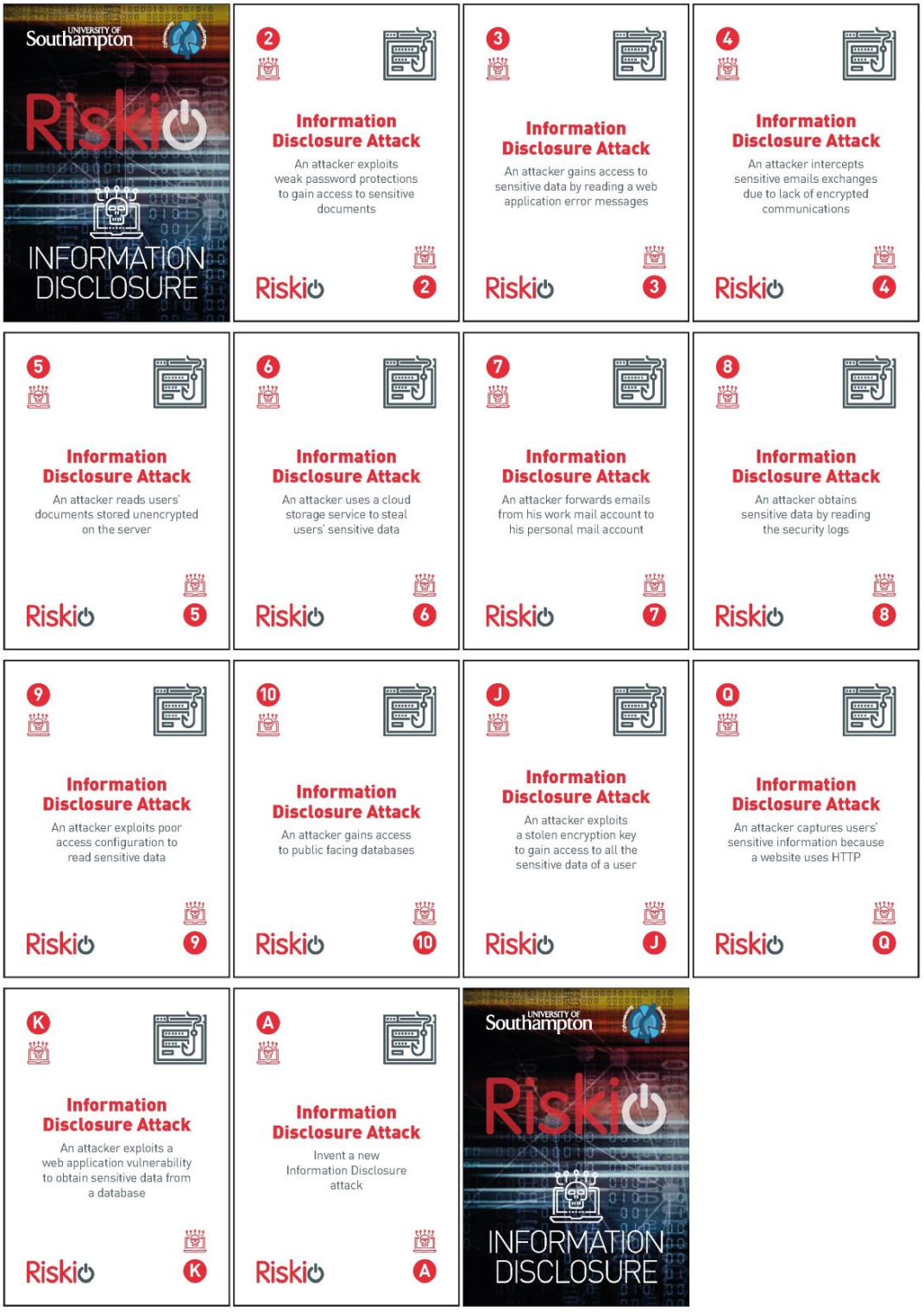


Figure B.4: Riskio Game Attack Deck - Information Disclosure Suit.

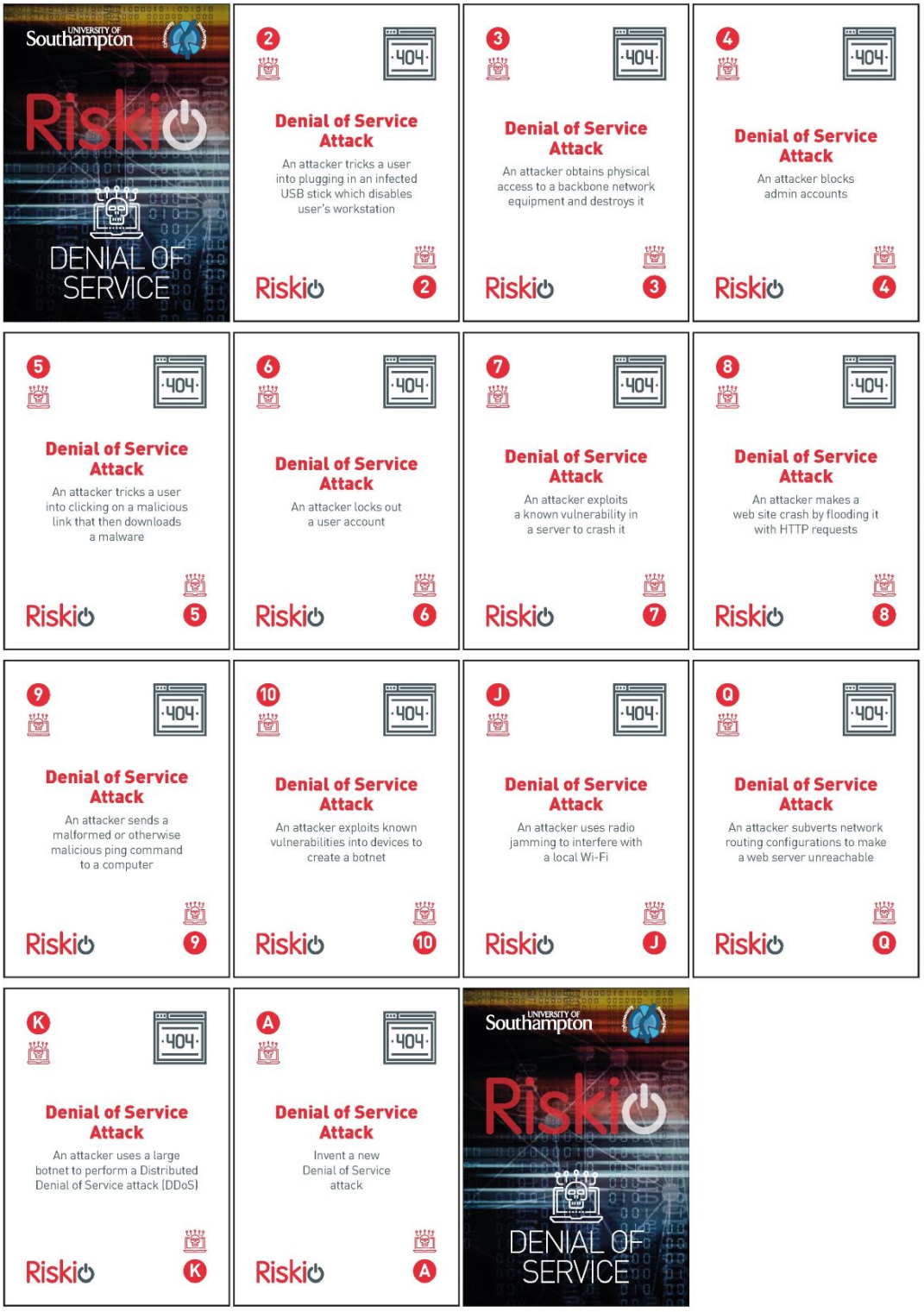


Figure B.5: Riskio Game Attack Deck - Information Denial of Service Suit.

Figure B.6: Riskio Game Attack Deck - Elevation of Privilege Suit.

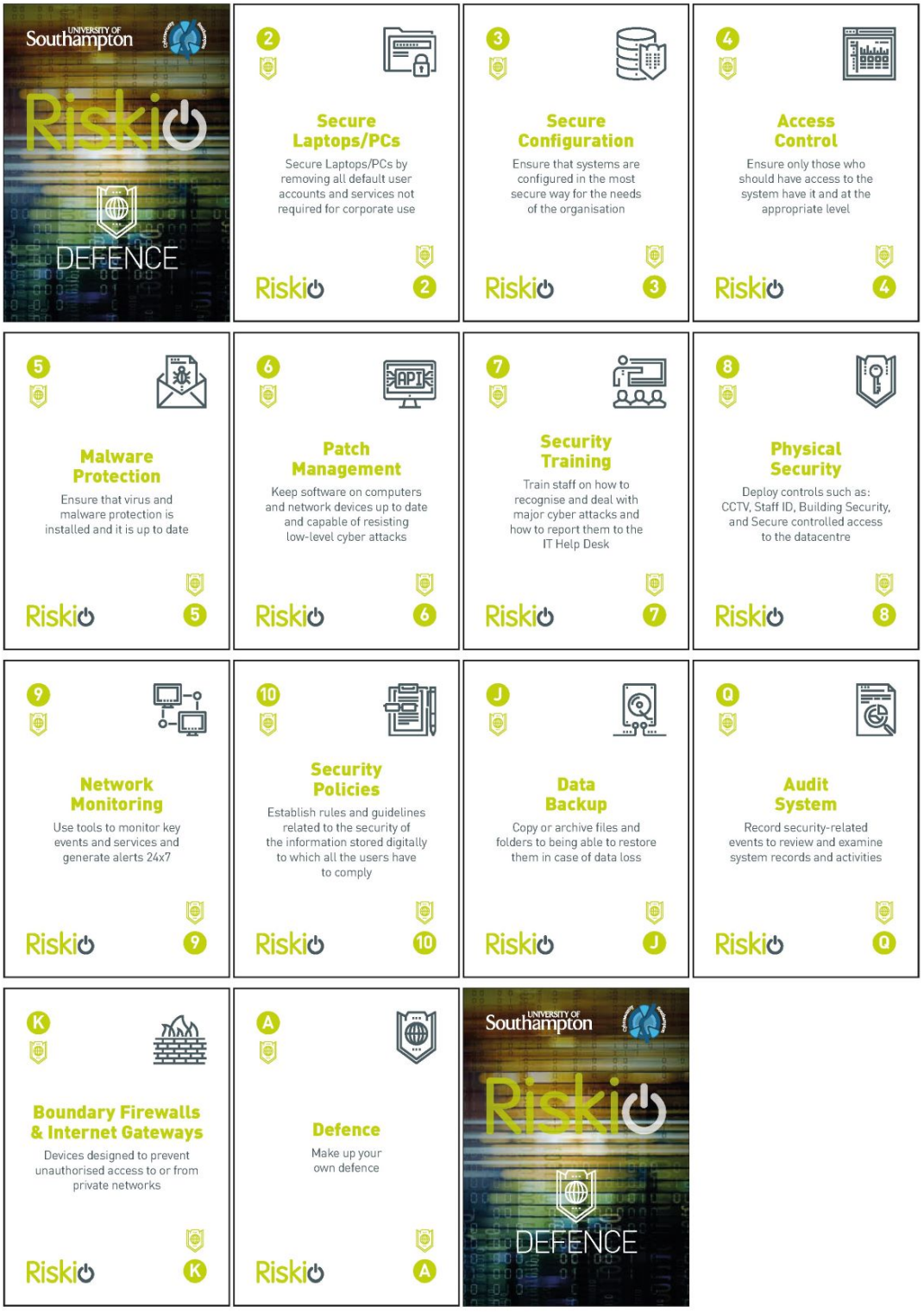


Figure B.7: Riskio Game Defence Suit.

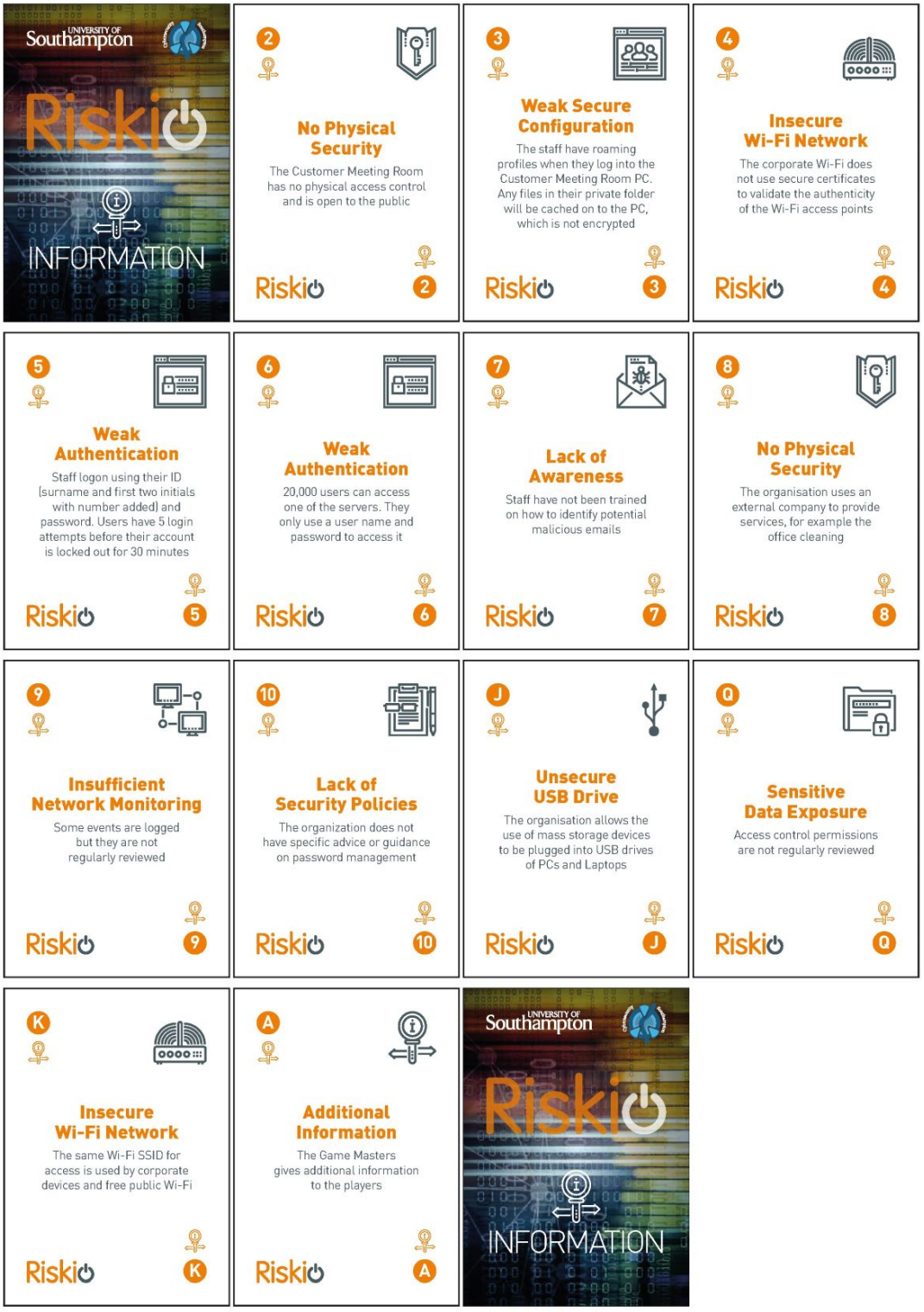


Figure B.8: Riskio Game Information Suit.

Appendix C

Participant Information Sheet ERGO 44919

Example of the participant information sheet given to all players of the Riskio playtests as identified in Section 5.2.

UNIVERSITY OF Southampton

Participant Information Sheet

Study Title: A card game to raise awareness of cyber security to identify threats and possible defences

Researcher: Mr Stephen Hart
ERGO number: 44919

Please read this information carefully before deciding to take part in this research. It is up to you to decide whether or not to take part. If you are happy to participate you will be asked to sign a consent form.

What is the research about? The research is for my PhD and the main aim of the research is to increase awareness in cyber security of c-level executives and senior managers.

To conduct the research, I have developed a card game that could be played by c-level executives and senior managers who have limited training in cyber and information security but understand their core business processes and varying levels depending on their experience and position in the organisation.

Why have I been asked to participate? We value your contribution as senior managers in your organisation to improve the Riskio game and increase the effectiveness of the cyber security learning experience in playing the game.

What will happen to me if I take part? You will be asked to complete a questionnaire before the game on your background to security awareness and a second questionnaire after the game on your assessment of the game. Your responses will be anonymised and will not be attributed to you or any individual.

Are there any benefits in my taking part? The game is designed to increase the players cyber security awareness to identify threats and find defences against the identified threats.

The Riskio Game will be released and made available online and licensed under the Creative Commons Attribution 3.0 United States License http://creativecommons.org/licenses/by/3.0/us/. You will be able to download the game and have the advantage to have played with the game creators.

Are there any risks involved? There are no risks involved in playing the game. However, if a participant mentions something during the game and asks for this not to be used, this will have excluded from the research.

Will my participation be confidential? Your participation will be confidential, and any personal data will be anonymised. If any participant mentions something which could identify an organisation or individual this will not be used in the research and where feasible this will be securely destroyed. The questionnaire at the before and at the end of game will not use your real name and will be using "unlinked anonymity".

What should I do if I want to take part? Please tell the course tutor if you do not want to take part in the research.

What happens if I change my mind? During the game play if a player decides they do not want to continue the data collecting part of the game will stop and all material will be securely destroyed.

What happens to the score sheets used in the game play? The score sheet is kept to record which cards were played in the game play and any additional comments made. They will not be linked back to you as data subject and any identify data will not be recorded.

What will happen to the results of the research? The research is in its first year and the final thesis will be published and contain anonymised research data. The anonymised research data including the transcribed notes will be kept for a minimum of 10 years for staff and postgraduate research students, as per University of Southampton policy.

The research may also be published in scientific journals and other relevant publications. This could happen over the next few years and post publication of the thesis.

Where can I get more information? If you require any additional information please see main contacts below:

Contact for research student: ***Redacted***

What happens if something goes wrong? If you have any concerns or complaints, please contact below who is independent of the research study. The University has insurance in place to cover its legal liabilities in respect of this study.

The Research Integrity and Governance Manager (023 8059 5058, rgoinfo@soton.ac.uk).

Thank you.

Thanks for taking the time to read this participant information sheet and considering taking part in the research to improve cyber security awareness in c-level executives and senior managers.

Appendix D

Consent Form ERGO 44919

Example of the consent form required by all players of the Riskio playtests as identified in Section 5.2.

UNIVERSITY OF Southampton

CONSENT FORM

Study title: A card game to raise awareness of cyber security to identify threats and possible defences

Researcher name: Mr Stephen Hart

ERGO number: 44919

Please initial the box(es) if you agree with the statement(s):

Question	Initials
I have read and understood the information sheet (18/09/2018) version 1.1 of participant information sheet) and have had the opportunity to ask questions about the study.	
I agree to take part in this research project and agree for my data to be used for the purpose of this study	
I understand my participation is voluntary and I may withdraw for any reason without my rights being affected.	
I understand my responses will be anonymised in reports for the research.	
I understand I can withdraw my consent at any time up to the game finishes but will only be able to withdraw my answers to the questionnaires later by remembering my 4-digit random number as questionnaires are not linked to me as data subject as this is not required for data processing under article 11 GDPR.	
I understand that if I withdraw my consent later after the anonymised data has been published it will be impossible to have this deleted.	

Name of participant (print name) .....

Signature of participant .....

Date .....

Name of researcher (print name) .....

Signature of researcher .....

Date .....

Appendix E

Riskio Questionnaire 1 - Players Background

This questionnaire is to collect data about the background of the participants. The answers to this questionnaire are NOT used by any means to evaluate/grade them.
Please do not provide your real name as participant identifier. Please write the 4-digit random number as the participant identifier you will be given. This number will be used in questionnaire 2 after the game.

Participant identifier: _____ _____ _____ _____

1. **Which team/function area do you work in at your organisation?**
   You are currently:
   ☐ working in organisation IT Team
   ☐ working in organisation Operations Team
   ☐ working in organisation Risk / Assurance / Compliance team
   ☐ working in organisation Security Team
   ☐ working in organisation Finance Team
   ☐ working in organisation HR team
   ☐ working in organisation Information Management Team
   ☐ working in organisation as CEO
   ☐ other _____

2. **What is your highest level of education?**
   ☐ PhD
   ☐ MSc
   ☐ BSc
   ☐ Technical College etc.
   ☐ Secondary School

3. **What degree do you have?** Please specify degree

   _____

4. **How would you describe your level of expertise in cyber security?**
   Please choose only one of the following options:
   novice ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 expert

5. **How would you describe your level of knowledge in cyber attack trends?**
   Please choose only one of the following options:
   novice ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 expert

6. **Do you have any qualifications in Cyber Security or Information Technology?**
   ☐ PhD
   ☐ MSc
   ☐ BSc
   ☐ CISSP/CISM/CEH etc.
   ☐ None

7. **How would you describe your level of expertise in information technology?**
   Please choose only one of the following options:
   novice ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 expert

8. **How would you describe your level of expertise in physical building security?**
   Please choose only one of the following options:
   novice ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 expert

9. **How would you describe your level of expertise in risk assessments?**
   Please choose only one of the following options:
   novice ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 expert

10. **How would you describe your level of expertise in Microsoft STRIDE?**
    Please choose only one of the following options:
    novice ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 expert

Appendix F

Riskio Questionnaire 2 - Post Playing Game

This questionnaire (see Table F.1) is to collect your impressions about the Riskio Game. The answers to this questionnaire are NOT used by any means to evaluate/grade you.

Please do not provide your real name as participant identifier. Please use the 4-digit random number you used for questionnaire 1.

Participant identifier: _____ _____ _____ _____

Read questions carefully. The positive and negative statements of the questions are mixed. The questionnaire has an opposing statements format, so If you agree strongly with the statement on the left, check the leftmost box (1). If you agree, but less strongly, with the left statement, check box #2 from the left (2). If you agree with neither statement, or find them equally correct, check the middle box (3). If you agree, but less strongly, with the right statement, check box #2 from the right (4). If you agree strongly with the statement on the right, check the rightmost box (5).

Table F.1: Riskio Game Post Game Questionnaire assessment.

No		1 2 3 4 5	
	About Riskio Game		
1	I found playing the Riskio Game did not improve my knowledge of Cyber Security	☐☐☐☐☐	I found playing the Riskio Game improved my knowledge of Cyber Security
2	I found the Riskio Game difficult to learn	☐☐☐☐☐	I found the Riskio Game easy to learn

Continued on next page

Table F.1 – continued from previous page

No		1 2 3 4 5	
3	Overall, I think playing the Riskio Game does not provide an effective solution to the identification of cyber threats	☐☐☐☐☐	Overall, I think playing the Riskio Game provides an effective solution to the identification of cyber threats
4	If the game was adapted based on my organisation, I would not use the Riskio Game to identify cyber threats	☐☐☐☐☐	If the game was adapted based on my organisation, I would use the Riskio Game to identify cyber threats
5	Playing the Riskio Game did not help me find new threats that I could have found without playing the game	☐☐☐☐☐	Playing the Riskio Game helped me find new threats that I could have not found without playing the game
6	Overall, I think playing the Riskio Game does not provide an effective solution to the identification of cyber defences	☐☐☐☐☐	Overall, I think playing the Riskio Game provides an effective solution to the identification of cyber defences
7	If the game was adapted based on my organisation, I would not use the Riskio Game to identify cyber defences	☐☐☐☐☐	If the game was adapted based on my organisation, I would use the Riskio Game to identify cyber defences
8	Playing the Riskio Game did not help me find new defences that I could have found without playing the game	☐☐☐☐☐	Playing the Riskio Game helped me find new defences that I could have not found without playing the game
9	If I need to increase Cyber Security awareness in a future project at work, I would not use the Riskio Game	☐☐☐☐☐	If I need to increase Cyber Security awareness in a future project at work, I would use the Riskio Game
10	Overall, I found playing Riskio Game to be useless	☐☐☐☐☐	Overall, I found playing Riskio Game to be useful
11	For the executives and senior managers in my organisation playing the Riskio Game would not be a productive method for them to increase cyber awareness	☐☐☐☐☐	For the executives and senior managers in my organisation playing the Riskio Game would be a productive method for them to increase cyber awareness
12	Playing Riskio Game did not make me more productive in identification of cyber threats	☐☐☐☐☐	Playing Riskio Game made me more productive in identification of cyber threats

Continued on next page

Table F.1 – continued from previous page

No		1 2 3 4 5	
13	Playing Riskio Game did not make me more productive in identification of cyber defences (counter measures)	☐☐☐☐☐	Playing Riskio Game made me more productive in identification of cyber defences (counter measures)
	About Security Games		
14	I feel playing a security card game is not effective method to teach cyber security	☐☐☐☐☐	I feel playing a security card game is a effective method to teach cyber security
15	I feel playing a security card game is not effective method to identify cyber security threats in my organisation	☐☐☐☐☐	I feel playing a security card game is a effective method to identify cyber security threats in my organisation
16	I feel playing a security card game is not effective method to identify cyber security defences in my organisation	☐☐☐☐☐	I feel playing a security card game is a effective method to identify cyber security defences in my organisation

Appendix G

Riskio Attack and Defence Examples

Attack and Defence Examples for Games Master Only, see Table G.1.

Table G.1: Riskio Example Spoofing Attack and Defence.

Riskio Card	Spoofing Attack (Front of Card Description)	Actor Trigger Attack / Example Applied to Design	Defence (Can only play one card)
2	An attacker sends emails pretending they come from the IT Service	Employee (Unintentional) - The attacker could send an email requesting the user to log in to change password	Secure Configuration- Flag emails on the Email server so users can see they are external emails
3	An attacker tries possible passwords one by one until he finds the correct one	Cyber Criminals - The attacker knows the format you use for emails (first name, dot then surnames), tries names found on website with password guessing	Access Control – After five attempts lock the account for two hours
4	An attacker tricks users into visiting a malicious website	Employee (Unintentional) - The attacker has installed key logging software on work PC and anyone who uses it, the passwords are being sent to the attacker	Secure Configuration – Block websites that do not comply with security policy

Continued on next page

Table G.1 – continued from previous page

Riskio Card	Spoofing Attack (Front of Card Description)	Actor Trigger Attack / Example Applied to Design	Defence (Can only play one card)
5	An attacker tricks users into connecting to a rogue Wireless Access Point (WAP) thinking they were connecting to the corporate WAP	Employee (Unintentional) - The attacker acts as man-in-the-middle and can capture all passwords etc of the employee	Security Training – Train staff in the risks of mobile devices and connection to Wi-Fi access points
6	An attacker obtains a digital certificate of a trusted server to forge malicious communications	Cyber Criminals - The attacker can send emails to the corporate email server and the email server will verify it's from the company	Secure Configuration - Use of Certificates installed on both company and contractors Email Server
7	An attacker intercepts users' credentials over an encrypted communication link	Cyber Criminals - ARP spoofing (ARP Poisoning) - process of sending faked ARP messages in the network. The purpose of this spoofing is to associate the MAC address with the IP address of another legitimate host causing traffic redirection to the attacker host. This kind of spoofing is often used in man-in-the-middle attacks.	Secure Configuration – Use of secure Virtual Private Networks (VPN) that largely blocks your activity from ARP spoofing hackers.
8	An attacker steals users' credentials stored in clear text on a server	Cyber Criminals - Attacker could use these credentials to connect to the corporate wireless access point and access sensitive data	Secure Configuration – Ensure all password files are encrypted

Continued on next page

Table G.1 – continued from previous page

Riskio Card	Spoofing Attack (Front of Card Description)	Actor Trigger Attack / Example Applied to Design	Defence (Can only play one card)
9	An attacker steals users' credentials due to lack of an encrypted communication link	Cyber Criminals - Attacker could use these credentials to connect to - corporate router as a home user and access sensitive data	Access Controls – Remote workers need two-factor authentication to connect remotely using an RSA token.
10	An attacker sends an email targeting a specific user	Cyber Criminals - Attacker gathered information from corporate website and used this to create emails to target employees	Security Training – Train staff how to spot spear fishing emails.
Jack	An attacker looks over the shoulder of a user to steal their credentials	Cyber Criminals – Attacker can use mobile phone to record employee logging into the system	Security Training – Train staff to be aware of shoulder surfing
Queen	An attacker exploits a vulnerability in the process to recover or update users' credentials	Cyber Criminals - Attacker uses the password reset to gain access to a user's account	Access Control – Password reset requires user to call service desk and identify themselves.
King	An attacker exploits default admin credentials to access a server	Cyber Criminals - Attacker can remotely connect to the server and use the default password to access the server and take control	Secure Configuration – Company should have a security policy for new servers that includes changing any default passwords
Ace	Invent a new Spoofing attack		

Appendix H

Applying Activity Theory Six Steps

Table H.1: Activities and questions for clarifying the purpose of the activity system (Jonassen and Rohrer-Murphy, 1999).

Applying Activity Theory: Step One	
Clarify purpose of activity system.	
1.1 Understand relevant context(s) within which activities occur	Generate a list of problems that executives typically deal with. What participants or groups are involved in the successful completion of the activity? Where and when do those problems normally occur? Prioritise the list. Examine communications that surround the situation or activity.
1.2 Understand the subject, his or her motivations and interpretations of perceived contradictions in the system.	Generate a comprehensive list of subject-driven motives and goals for each of the groups involved that might drive the activity. What expectations are there of the performer? Who sets those expectations? Which might contribute to the dynamics of the situation under review? Interview persons directly and peripherally associated with activity to understand contradictions, overall factors that affect activity.

Continued on next page

Table H.1 – continued from previous page

Applying Activity Theory: Step Two	
Analyse the Activity System.	
2.1 Define the subject	Who are the participants in the activity system? What are their roles? What are their beliefs? What is the expected outcome of the activity? What criteria will be used by the community to evaluate its utility? What are the implied rules or roles for each member of the group? What struggles did the group survive in order to reach its current state? What are goals-motives of the activity and how are they related to goals motives of others and society? What is the division of labour within the activity system? What perceived rewards await the subject if or when it accomplishes its goal?
2.2 Define the relevant community-communities	To what extent does the subject's work community impact the subject object pair? How mature is the group? How formally are the rules of interaction stated? What is the structure of social interactions surrounding the activity? How might conflicts that originate in other communities affect participant interactions? How do other communities in which participants are involved view this task? Do they value the goals of the activity? What perceived rewards await the subject if or when it accomplishes its goal?
2.3 Define the object	What is the expected outcome of the activity? Is the end product a presentation, a report, a theory or a combination of these (or other) elements? What criteria will be used to evaluate the quality of the outcome? Its viability? Who will apply the specified criteria? How much credibility does that individual or group have with participants? How will completing the object move the participant toward fulfilling the intentions of the individuals? or the program?

Continued on next page

Table H.1 – continued from previous page

Applying Activity Theory: Step Three	
Analyse the activity structure.	
3.1 Define the activity itself	How is work being done in practice? Identify the activities in which subjects participate. How has the work (actions and operations) been transformed over time? What historical phases have there been on the work activity? What was the nature of the changes that occurred in different historical phases? What norms, rules, and procedures in the actions and operations have been documented? What forms of thought, "rationality types," or theoretical foundations have dominated the work and how have they changed? What do the workers think about them? What are goals-motives of the activity and how are they related to other concurrent goals? What are the contradictions, as perceived from the standpoints of all relevant subjects that drive this activity?
3.2 Decompose the activity into its component actions and operations	For each activity, observe and analyse the actions that are performed and by whom. Examples may include problem isolation, calling and managing meetings, developing operational plans, etc. For each action, observe and analyse the operations that subjects perform. Examples of operation include: note taking, calling on the telephone, sending messages, or setting up routine equipment.

Continued on next page

Table H.1 – continued from previous page

Applying Activity Theory: Step Four	
Analyse Mediators.	
4.1 Tool mediators and mediation	What tools might be used in this activity? How readily available are those tools to participants? What are the physical (instruments, machines) and cognitive (signs, procedures, methods, languages, formalisms, laws) tools used to perform activities in different settings and across activities (projects)? How have the tools changed over time? What models, theories, or standardized methods will guide this activity? How might participants use these? Is their use flexible, or is adherence required?
4.2 Rule mediators and mediation	What formal or informal rules, laws, or assumptions guide the activities in which people engage? How might these rules have evolved (formal-informal, internal-external)? Are they task-specific? How widely understood are these rules?
4.3 Role mediators and mediation	Who traditionally has assumed the various roles? How does that affect work group assignments or breakouts? How do these roles relate to the individual's non-academic experiences? What forces drive the role changes? How much freedom will individuals have to force others to take on new or different roles within the work group?

Continued on next page

Table H.1 – continued from previous page

Applying Activity Theory: Step Five	
Analyse the Content.	
5.1 Internal or subject driven contextual bounds	What are the beliefs, assumptions, models, and methods that are commonly held by working groups? How do individuals refer to their experiences in other work groups? What type of language do they use? What tools did they find (un)helpful in completing those projects? How willing are they to use them again? To try new tools in similar contexts?
5.2 External or community driven contextual bounds	How much freedom do individuals have about entering a work group? What is the structure of the social interactions surrounding the activity? What activities will be considered to be critical (i.e., assessed, measured, or graded)? What type of limitation will be placed on this activity by the company or outside agencies? How are the tasks organized among the members of the aggregate who are working toward the object? Will these structures be dictated or allowed to emerge from within each group? How are tasks divided or shared among participants? Who does what? How flexible is the division of labour? How will these roles and their contribution be evaluated (by evaluator or participants)? Is there a difference between the implied rules-roles for each member of the group and those that are formally stated? What formal or informal rules, laws, or assumptions guide the activities in which people engage? To what degree will the groups be expected to explicitly state those?

Continued on next page

Table H.1 – continued from previous page

Applying Activity Theory: Step Six	
Analyse Activity System Dynamics.	
6.1 What are the inter-relationships that exist within the components of the system?	What are the dynamics that exist between the components of the activity system? How formal-informal are the relationships described? Are there contradictions or inconsistencies within the needs of this population and the goals of these learning activities? How do the individuals perceive these goals, particularly vis-a-vis their own successes and their perceptions of what has led to those successes?
6.2 How formally established are those relationships?	How formally will the relationships between members be determined? What are the drivers of change? How lasting and permanent are these changes? How accepted are those relationships perceived within the framework of the larger graduate school culture?
6.3 How have those inter-relationships changed over time?	What factors have driven the formation of work groups within this population in the past? How lasting and permanent have these groups been in the past? What factors kept those groups together or drove those groups apart?

Appendix I

MOTENS Model Case Study for Participants

Problem Statement

Although there is consensus on the potential use of Serious Games (SGs) to teach cyber security and with examples of research that evidence the benefit of SGs there is no consensus on the methodology to design the SGs to identify the pedagogical elements of the game that map to the game mechanics and learning objectives. MOTENS is a pedagogical model to support the design of serious cyber games to achieve their stated learning objectives.

About this Case Study This case study is in four sections:

- **Section 1** - Brief background to motivation for cyber serious games design
- **Section 2** - Summary of the MOTENS Model
- **Section 3** - Brief high level explanation how to use the MOTENS Model using a serious cyber game called *'Riskio - A Serious Game for Cyber Security Awareness and Education'*
- **Section 4** - Reviewer Opportunity for Feedback

Section 1: Brief background to motivation for cyber serious games design

The increase successful cyber attacks where the organisation could have easily defended itself is an example in some cases where traditional cyber training has failed and serious cyber games can provide an active learning environment as an effective tool to increase cyber security training and awareness and reduce successful attacks that target employees of an organisation. Serious cyber games can also be used in software development to elicit security requirement by identifying vulnerabilities and mitigate early in the software development life-cycle. Serious cyber security games are built on the same principles as other serious games, see Figure I.1.

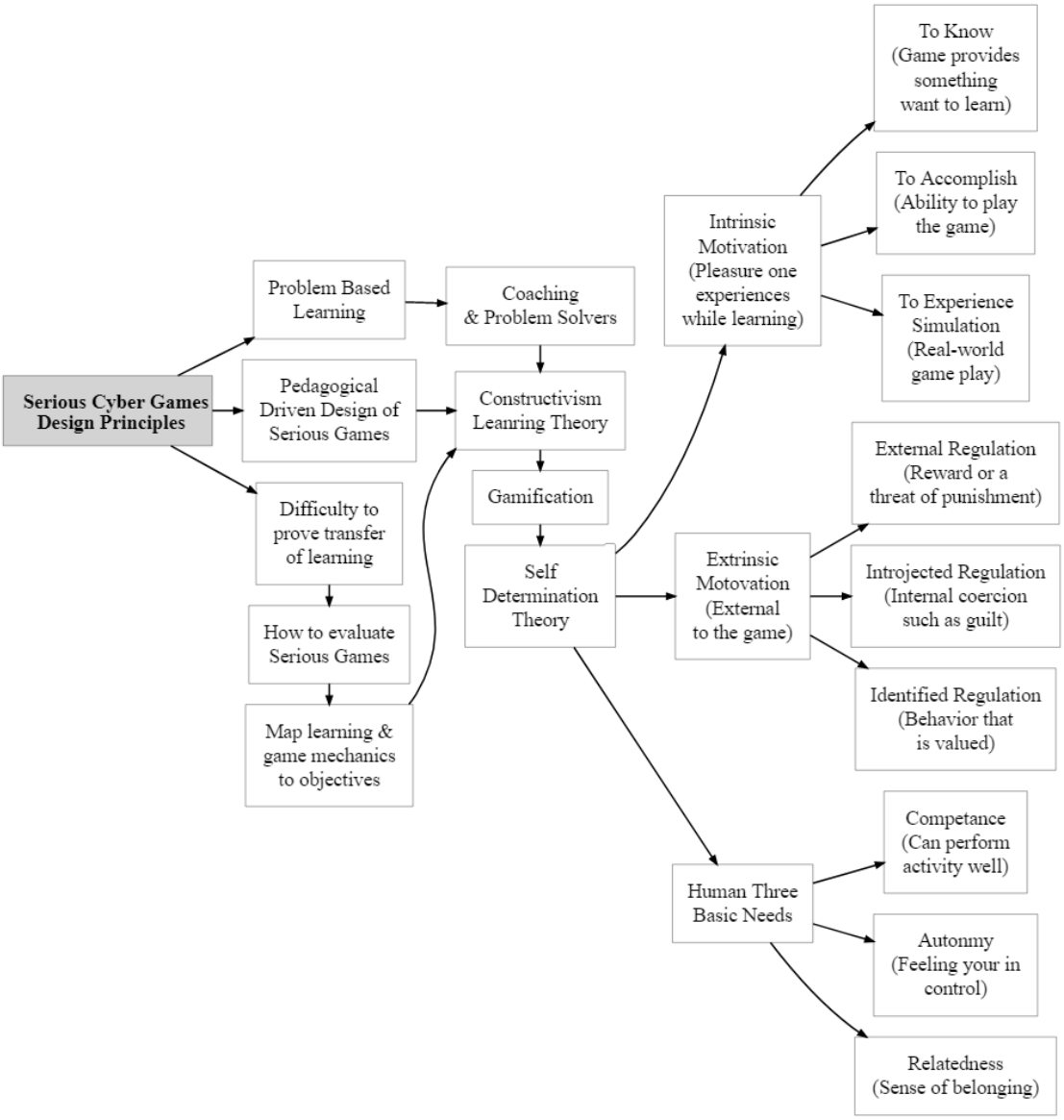


Figure I.1: Serious Cyber Games Design Principles

The traditional approach to education does not present problems to students but presents content to resolve problems. Three areas that are driving the change to *'problem-based learning'*. The first is an increasing demand to bridge the gap between theory and the real world. The second is the increase in information and accessibility to the information. The third is an emphasis on solving real-world problems. The move to problem-based learning will also require the shift in three loci of educational preoccupation: 1a) content coverage to 1b) problem engagement; 2a) from lecturer to 2b) coach; and 3a) from passive student learning to 3b) problem solvers, see Figure I.2.

Section 2: Summary of the MOTENS Model

The MOTENS model, see Figure I.3 was created based on the gaps identified in the current models for pedagogical assessment of serious games. The model is designed to assist the design

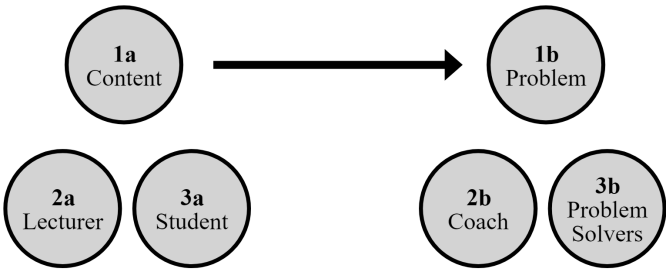


Figure I.2: Model Curriculum Shift

of serious cyber games.

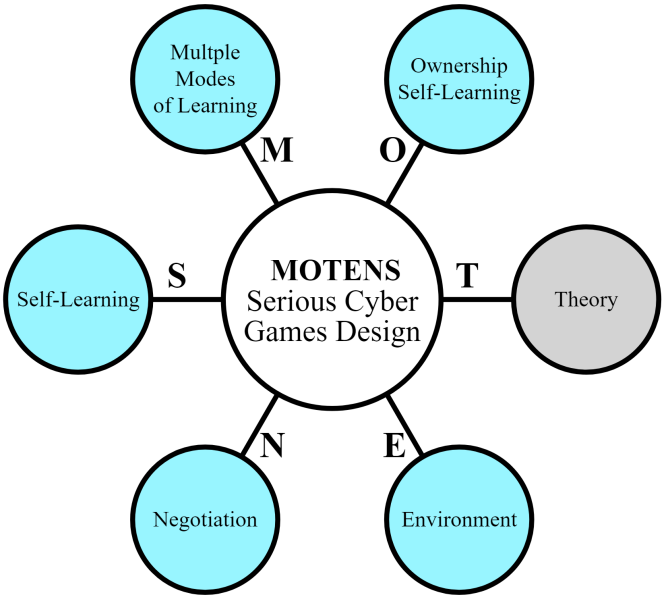


Figure I.3: MOTENS Model Detail

The MOTENS model is made up of six high-level components, five of the components can be directly linked to the games design/mechanics and one component 'Theory' is the supporting theory of the design including players motivation.

Figure I.4 shows the MOTENS model in more detail and the folders numbered D1 to D13 are linked to games design and boxes T1 to T5 are the theory that supports the design.

To design and create a serious cyber game the proposed model takes you through the following design stages: **Stage 1**: Target Game Players to identify and segment your target players into *non-gamers* and *gamers*. **Stage 2**: What game you want to create, decide category either Secure Software development or Security Awareness and Education and then decide the types of serious game: Card Games, Computer Games; Board/Table Games; or Speciality Games. Decide if your game will have a games master. **Stage 3:** Create initial MOTENS Design/Mechanics map. **Stage 4**: Design the Game, create the game using MOTENS model. **Stage 5**: Test and Evaluate by testing the game by playing and changing design/mechanics if required from player feedback.

Multiple Modes of Learning	The game mechanics that provide opportunities to learn a wide range of attacks and defences with players from different backgrounds.
Ownership Self-Learning	Provide different game scenarios to meet learning objectives.
Theory	The theory that supports the design.
Environment	Create a gameplay for players in a game setting they understand and appropriate learning environment.
Negotiation	Change the role from teacher to coaching not lecturing and from content delivery to problem-based learning.
Self-Learning	To create self-learning by use of problem-based learning; learning hierarchy; and build on players current knowledge.

Stage 1: Target Game Players (Segmentation)
The suggestion is that games designers should consider segmentation based on the two main categories of *non-gamer* casual player and *gamer* experienced game player. Using this simple segmentation group the target game players into two groups *non-gamer* and *gamer* or on a continuum between these.

Stage 2: What game you want to create
Figure I.5 shows examples of serious cyber games by category and type. It should be noted that MOTENS model is not suitable for Speciality Games for Secure Software Development.

Stage 3: Map of MOTENS Design/Mechanics
In this stage create a map of the MOTENS 13 design components the game you are designing mapped to the target players grouped by *non-gamers* and *gamers*. This will assist in stage 4 where decisions are made which game mechanics should be chosen as a balance to meet all target players requirements.

Stage 4: Designing the Serious Cyber Game
Following deciding the game type in stage 2, now the game design goes through the following steps mapped to the MOTENS detail model, see Figure I.4 and using map created in stage 3. This process of selecting the game design/mechanics can be iterative:

Step 1: Game Design - Initial Decisions (T1), (T3), & (T4)

(a) Select Threat Model (D3)
(b) Select Defence Framework (D5)
(c) Design/Graphics (D6)
(d) Document target players knowledge: Playing Games (D11); Cyber Knowledge (D11)
(e) Select Attacks & Defences related to target players (D12)
(f) Real-world problems to target players (D13)

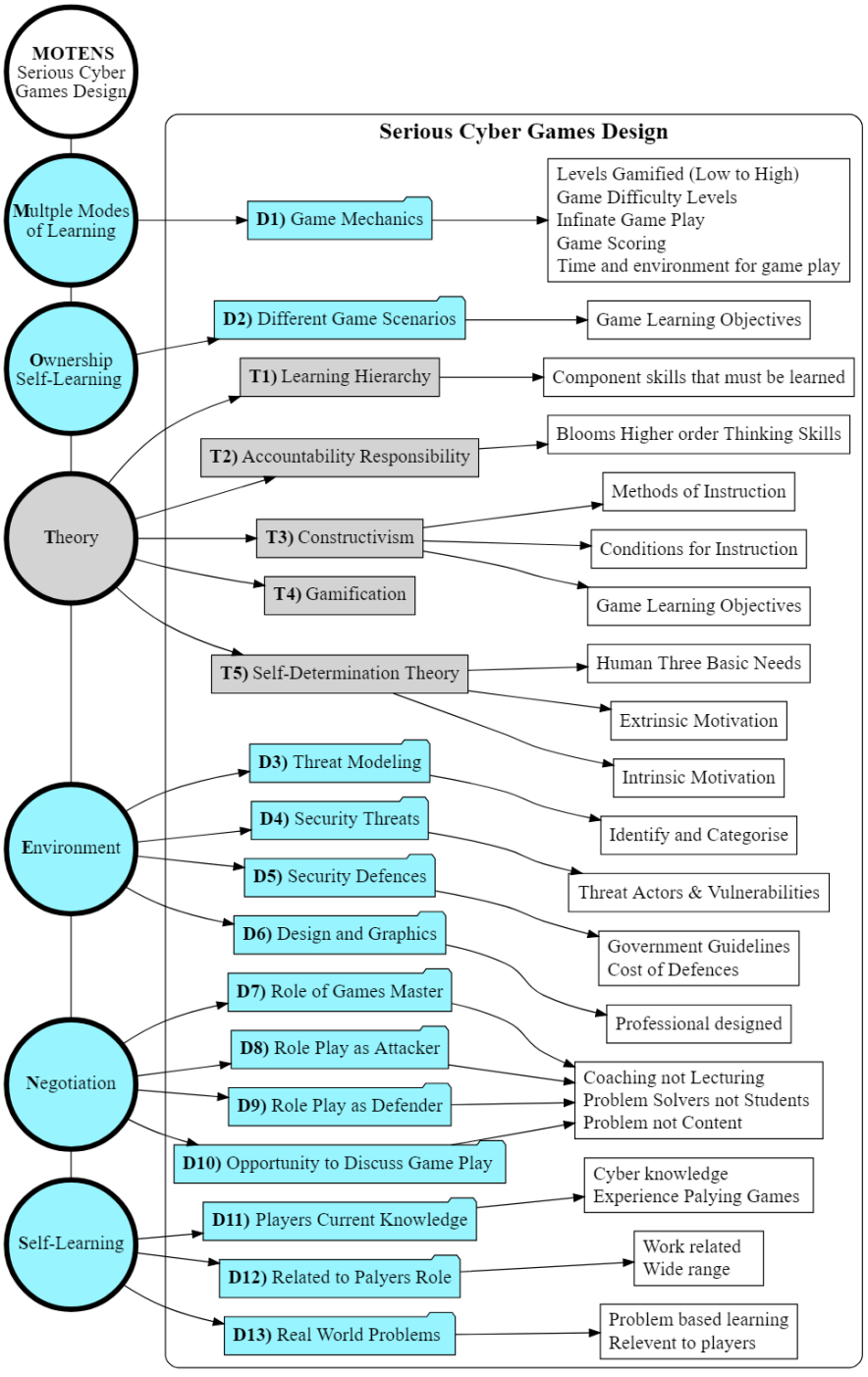


Figure I.4: MOTENS Model Detail

Step 2: Pre-Gameplay (T3), & (T4)

(a) How players understand threat model (D3) & (D7)

(b) Games setup (D2)

(c) How players understanding rules of the game (D8)

Step 3: Gameplay (T1), (T2), (T3), (T4), & (T5)

(a) Create map of stages of the gameplay (D1), (D4). (D7), (D9), (D10) & (D11)

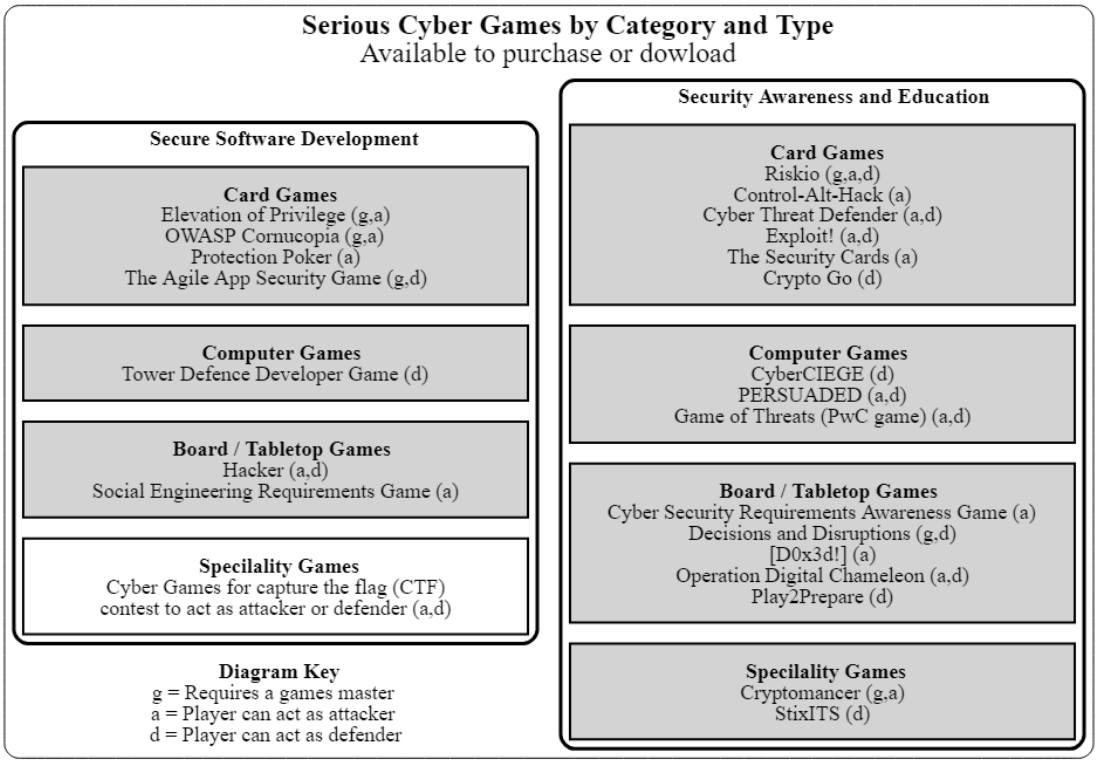


Figure I.5: Cyber Games by Categories

Step 4: Game End (T2), & (T3)

(a) Opportunity to discuss gameplay via group discussion on online blog etc. (D10)

Step 5: Review and Test Design

(a) Create map of MOTENS design/game mechanics to Non-Gamers and Gamers

(b) Create map of MOTENS design/game mechanics to game design and MOTENS theory

(c) Using maps created verify selected game mechanics meets game target groups requirements and game objectives

(d) Test gameplay and iterate through the steps as required

Stage 5: Test and Evaluate

The game can be played with real players to test the design and make changes before the final assessment. The last stage when the game is ready uses the Technology Acceptance Model to test the efficacy of the game by testing, Perceived Ease of Use, Perceived Usefulness and Intention to Use, see Figure I.6.

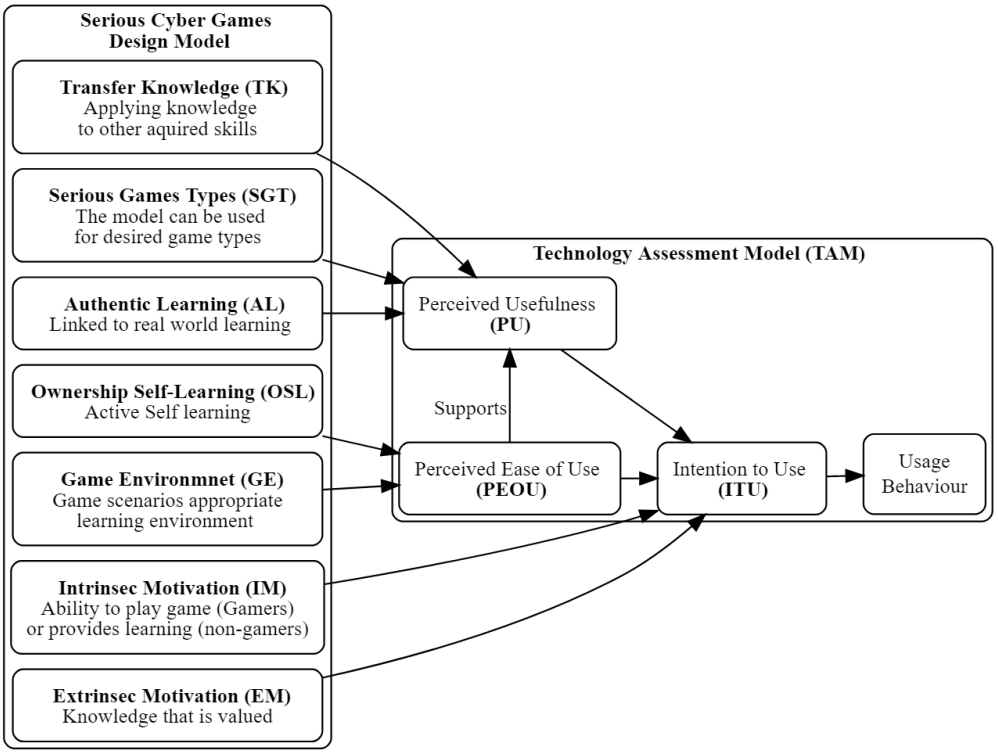


Figure I.6: TAM Model linked to MOTENS Model

Section 3: Brief high level explanation how to use the MOTENS Model using a serious cyber game called *'Riskio - A Serious Game for Cyber Security Awareness and Education'*

Stage 1: Target Players (Segmentation)

Riskio primary role is to educate employees on the risks coming from cyber attacks and best strategies to defend against them. The primary audience was *employees* with no technical background and secondary audience was university *students* who are studying in the field of cyber security. The primary audience was identified as mainly *non-gamers* and secondary audience students as *gamers*.

Stage 2: Type of Game

In the Riskio example, we decided to create a *Card game for Security Awareness and Education*, see Figure I.5. The next step we decided that Riskio needed a games master.

Stage 3: MOTENS Design Initial Map

In stage 3 when deciding the gameplay and mechanics a balance must be made to meet the game objectives and the target players requirements, see Figure I.7. In this example, we have identified six differences between the two target groups for Riskio in the initial assessment. Example: D1) Game Mechanics - Employees would not like game scoring, whereas students would like game scoring. In stage 4 must consider the initial differences identified.

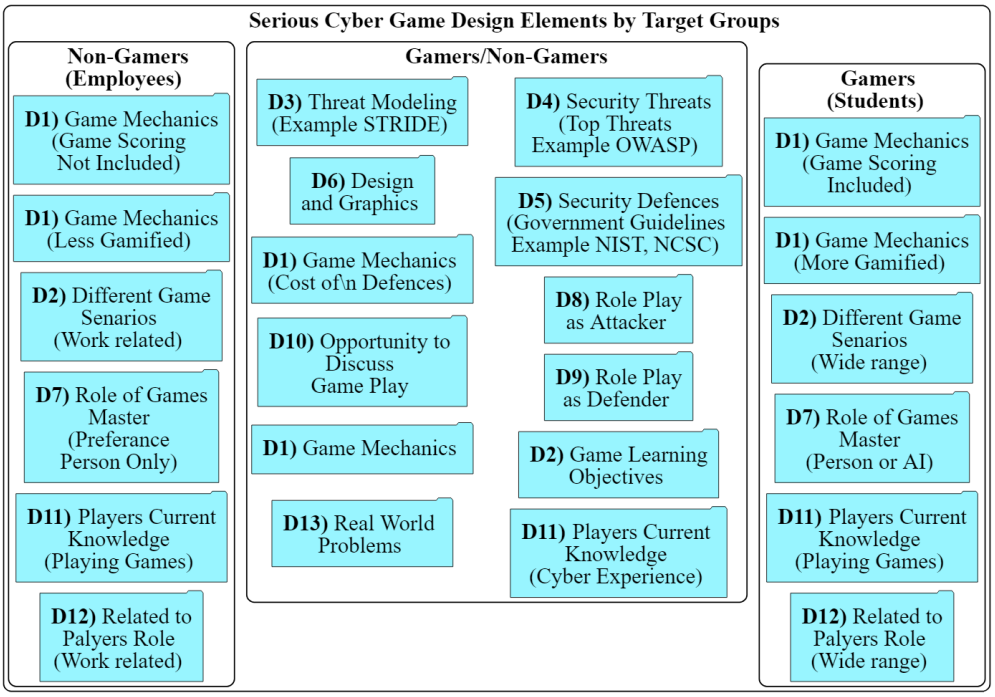


Figure I.7: Serious Game Elements

Stage 4: Design Gameplay/Mechanics

In this stage you will be deciding game mechanics, an example in Figure I.8 is choice in Riskio of players selecting their STRIDE suit or random selection of the STRIDE suit. The intrinsic motivation is different, the *Employees* (non-gamers), would prefer to select the STRIDE suit, whereas the *Students* (gamers) would prefer higher gamification and random selection. The theory from self-determination theory (STD) applied to this is that the intrinsic motivation for employees is they want to learn whereas for students they want to accomplish the game. This is an example of using the MOTENS model to link game design/mechanics to game theory.

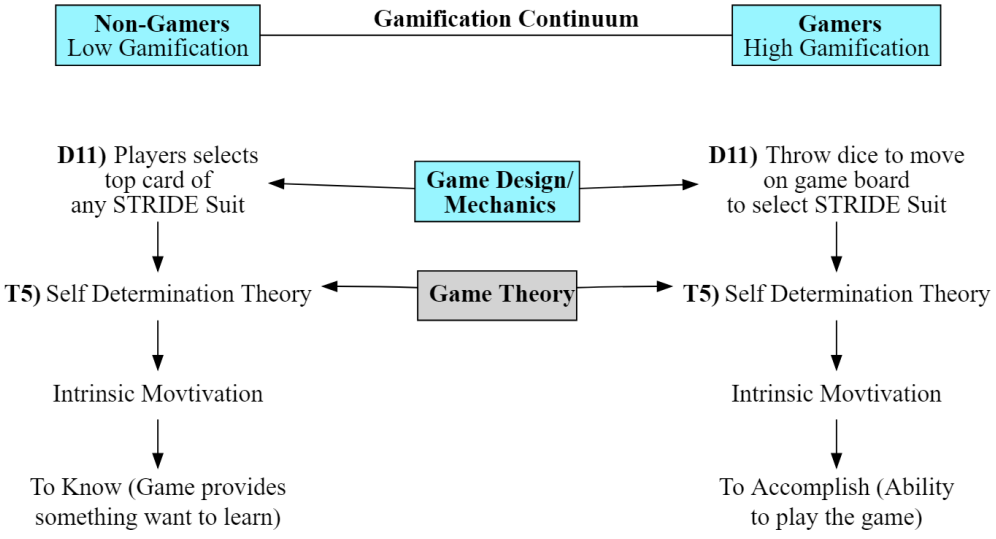


Figure I.8: Gamification

The game is designed in four steps:

Step 1 - Game Design Initial Decisions - see Figure I.9

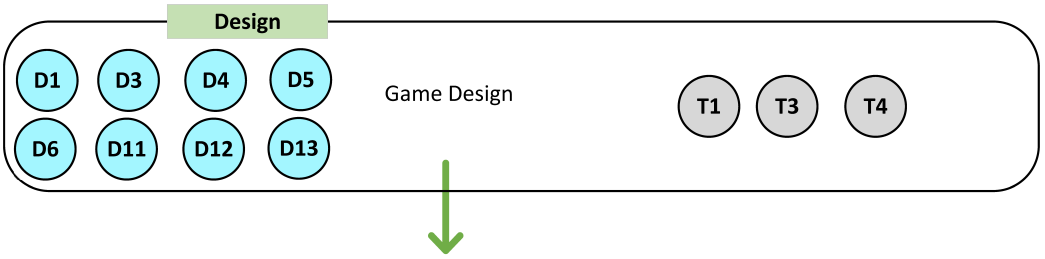


Figure I.9: MOTENS Design Riskio - Game Design Decisions

Gameplay 1 ***Game Design***

D1) *Game Mechanics:* Changeable game board

D3) *Threat Model:* The use of Microsoft STRIDE threat model

D4) *Security Threats:* Attacks cards that cover a wide range of attacks, categorised by selected Threat Model Microsoft STRIDE (six decks of attack cards one for each STRIDE category)

D4) *Security Threats:* Information Deck of Cards, to be used by games master to introduce new types of threats and vulnerabilities

D5) *Security Defences:* Defence cards that cover a wide range of defences from industry and government standards

D6) *Design & Graphics:* Game cards professional designed and high-quality card to simulate real game

D11) *Players Current Knowledge:* Students limited or no work experience; employees not gamers

D12) *Related to Players Role:* Employees work experience in relevant industry; and Students want to experience a wide range roles from different industries

D13) *Real World Problems:* Employees work related; and Students wide range of threats and vulnerabilities

Step 2 - Pre-Gameplay - see Figure I.10

Gameplay 2 ***Pre-game stage***

D7) *Role of Games Master:* The games master gives tutorial on Microsoft STRIDE

D2) *Different Game Scenarios:* 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 scenario is based on a fictional University Fees Office

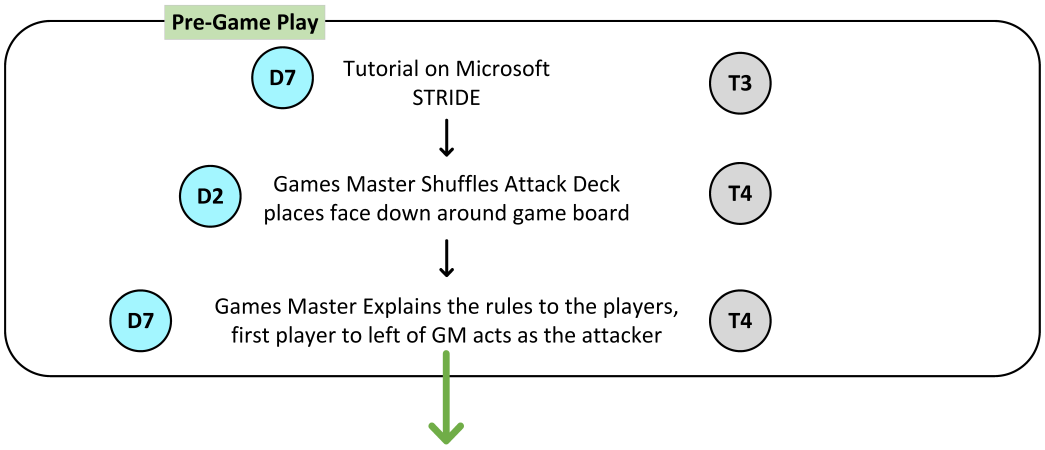


Figure I.10: MOTENS Design Riskio - Pre-Gameplay

D7) *Role of Games Master:* The games master gives demonstration of Riskio with example of attack and defence

Step 3 - Gameplay - see Figure I.11

Attack Stage

Gameplay 3 **D8)** *Role Play Attacker:* Player can see a vulnerability known to them on the board and selects from appropriate STRIDE category

Gameplay 4 **D11)** *Players Current Knowledge:* Player explains the attack

Gameplay 5 **D1)** *Game Mechanics:* Create a sense of urgency

Gameplay 6 **D11)** *Players Current Knowledge:* Player can select any defence card

Defence Stage

Gameplay 7 **D9)** *Role Play Defender:* All the players explain how their defence will work and why

Choice: Next player: Gameplay 8; Game Master Attacks: Gameplay 9; or Game ends: Gameplay 11

Gameplay 8 **D1)** *Game Mechanics:* Repetition, players have several turns at attacking and defending

Games Master Attack Stage

Gameplay 9 **D4)** *Security Threats:* Games master uses information deck to introduce new threats

Gameplay 10 **D7)** *Role of Games Master:* Games master acts as attacker and players defend

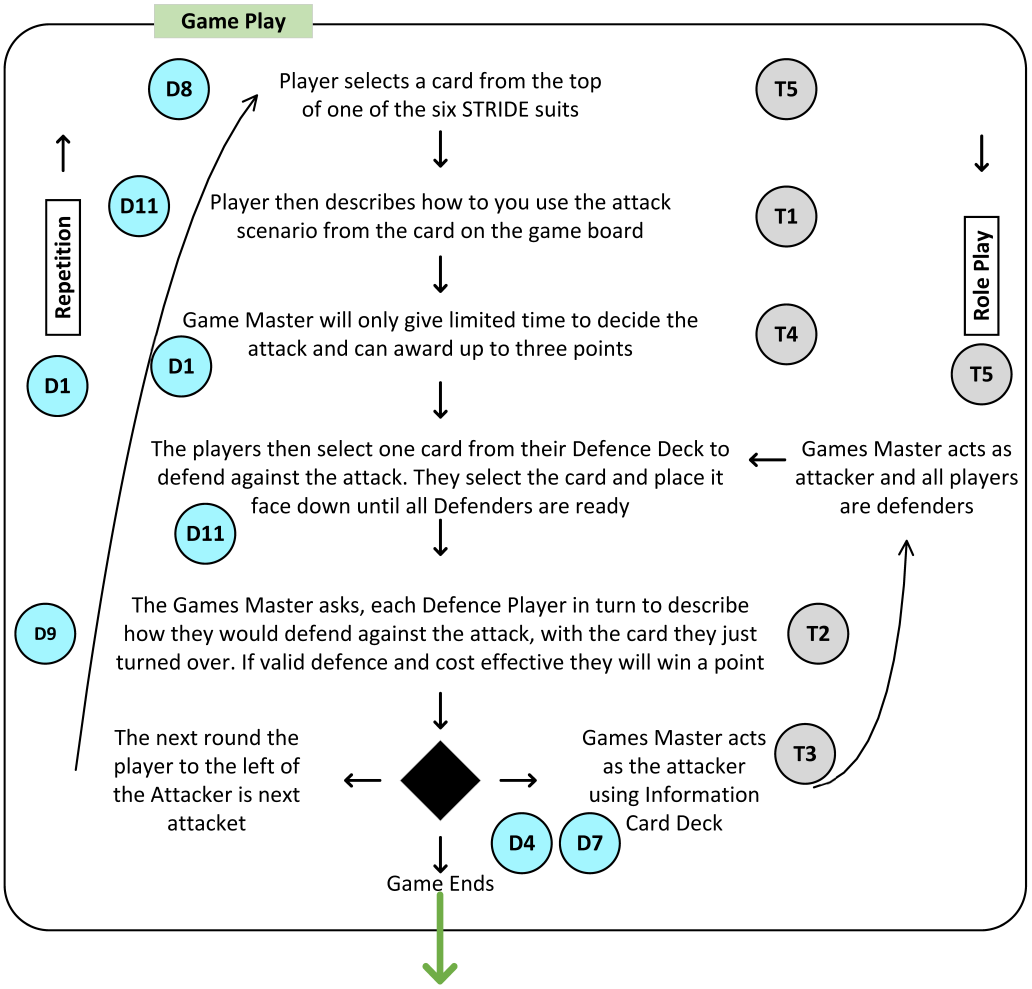


Figure I.11: MOTENS Design Riskio - Gameplay

Step 4 - Game End - see Figure I.12

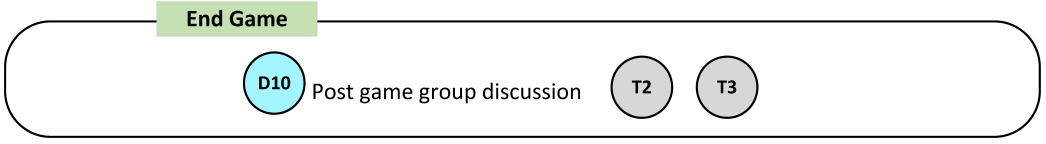


Figure I.12: MOTENS Design Riskio - Game End

End Game

Gameplay 11 **D10)** *Post game group discussion:* The players have opportunity to discuss what they learnt and ask each other and games master questions

Step 5 - Continuous Review and Test Design

The feedback when testing can be used to test different game design/mechanics. This give opportunity to test various options to find the most effective and also create alternative rules to meet objectives of both non-gamers and gamers.

Section 4: Reviewer Opportunity for Feedback

'Thank for your time and for your assessment and feedback on the MOTENS Model for Serious Cyber Games Design. For information the questions are scaled 1 to 5 using the Technology Acceptance Model (TAM) to assess: Perceived Usefulness (PU); Perceived Ease of Use (PEOU); and Intention to Use (ITU), see Figure 7.5.

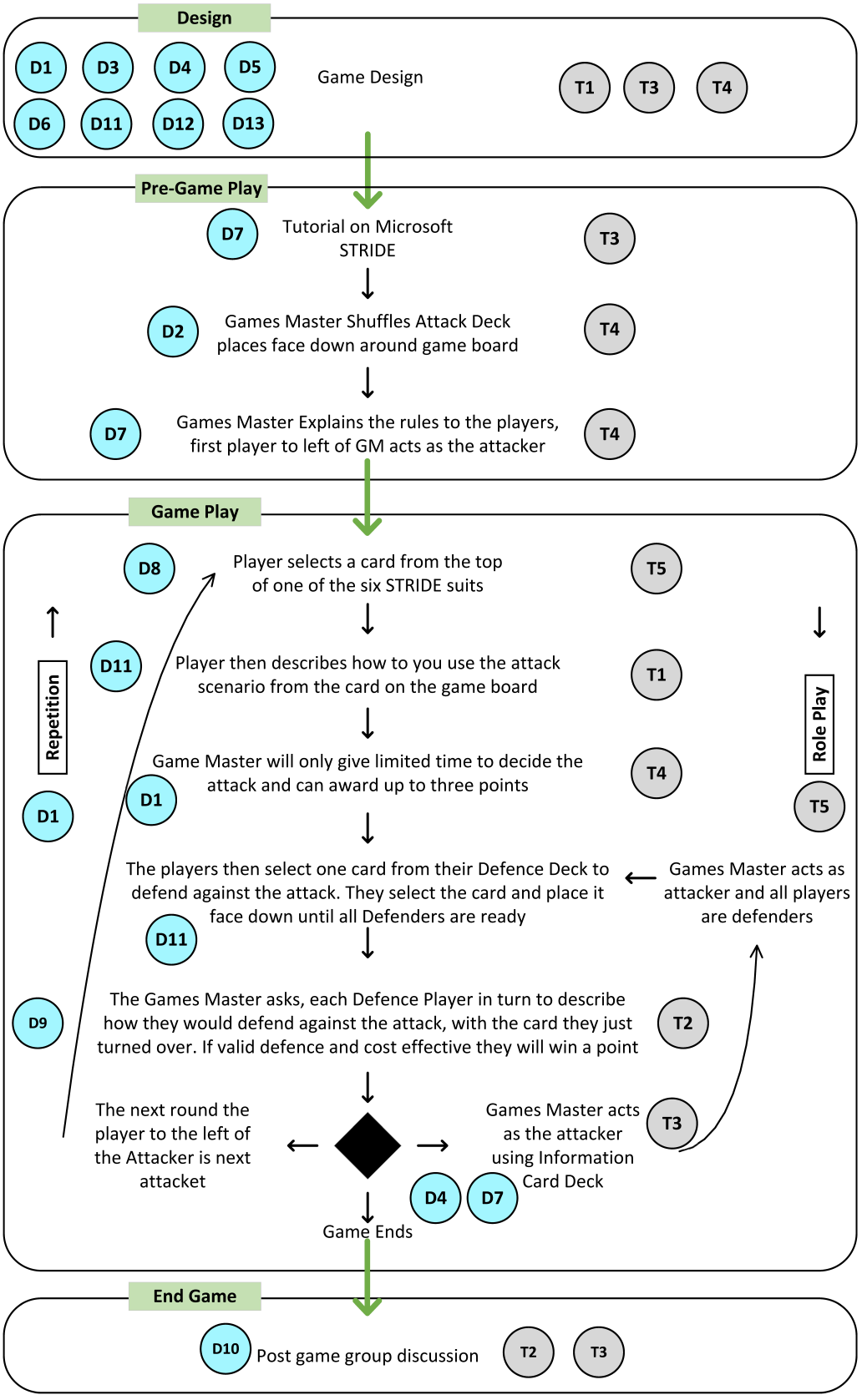


Figure I.13: MOTENS Design Riskio

Appendix J

MOTENS Model Questionnaire

This questionnaire is to collect your impressions about the proposed pedagogical design model for serious cyber games. The answers to this questionnaire are NOT used by any means to evaluate/grade you. The questionnaire is in four sections, the first on types of cyber games covered by the model and the last three are based on the Technology Acceptance Model (TAM): Perceived Ease of Use (PEOU), Perceived Usefulness (PU) and Intention to Use (ITU).

Please do not provide your real names participant identifier. Please use the 4-digit random number.

Participant identifier: _____ _____ _____ _____

Which team/function area do you work in at your organisation?
☐ Working for a University as Professor; Associate Professor or Lecturer
☐ Working for a University in the Research Department
☐ Working for UK Government in the Research Department
☐ Working for Organisation in the Research Department
☐ PhD Student
☐ Other Please state _____

What is your knowledge of Riskio game? (Tick all that apply)
☐ None
☐ I have played the Riskio game as a player
☐ I have played the Riskio game as a games master
☐ I have read the paper published by Elsevier in Computers & Security

Read each question carefully as each question can be positive or negative.
If you strongly disagree with the statement, check the leftmost box (1).
If you disagree, but less strongly, with the statement, check box #2 from the left (2).
If you agree with neither statement, check the middle box (3).
If you agree, with the statement, check box #4 from the right (4).
If you agree strongly with the statement, check the rightmost box (5).

Table J.1: MOTENS Illustrative Case Study - Questionnaire Cyber Games Design Model.

No	Question	Strongly Disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
	Section 1 – Perceived Relevance in Serious Cyber Games Development (PU)					
1	I found the model covered all types of serious cyber games I expected.	☐	☐	☐	☐	☐
2	I feel that the model would be useful in the design of the all the types of games: Card Games; Computer Games; Board Games; and Speciality Games (Education & awareness only for this type), see Figure I:5 in Case Study.	☐	☐	☐	☐	☐
	Section 2 – Perceived Ease of Use (PEOU)					
3	I found the MOTENS model would be easy to use.	☐	☐	☐	☐	☐
4	I found the MOTENS model was able to match learning objectives to serious games mechanics.	☐	☐	☐	☐	☐
	Section 3 - Perceived Usefulness (PU)					
5	I think using the MOTENS model to design serious cyber games will improve learning outcomes and give greater chance to meet desired learning objectives of serious cyber games design.	☐	☐	☐	☐	☐
6	I feel playing serious cyber games is an effective method to teach cyber security awareness and education and secure software development.	☐	☐	☐	☐	☐

Continued on next page

Table J.1 – continued from previous page

	Section 4 – Intention to Use (ITU)					
7	I would recommend the MOTENS model to anyone designing a serious cyber game.	☐	☐	☐	☐	☐
8	Overall, I think the MOTENS model will be useful to design cyber games to meet intended objectives and I would use it to help to design serious cyber games.	☐	☐	☐	☐	☐
	Please enter any additional comments					

Participant Information - What is the research about?

The research is for my PhD and the main aim of the research is to educate employees on the nature of the risks coming from cyber attacks and the best strategies to defend against them. To conduct the research, I have developed a card game called Riskio that could be played by c-level executives and senior managers who have limited training in cyber and information security but understand their core business processes and varying levels depending on their experience and position in the organisation. The next stage is to create a framework that could support the design and the evaluation of serious games to educate people on cyber security concepts that reconciles both principles from serious games design and educational theories. If you require any additional information please see contact information below:

Contact for research student: Mr Stephen Hart

Email: stephen.hart@soton.ac.uk

University of Southampton: www.ecs.soton.ac.uk/people/sjh1n15

Riskio Website: https://www.riskio.co.uk/

Privacy Statement

Your participation will be confidential, and no personal data will be collected. If any participant mentions something in comments section which could identify an individual this will not be used in the research and where feasible this will be securely destroyed.

Appendix K

MOTENS versus LM-GM Model Questionnaire

Version 3.1

MOTENS Model Questionnaire Models to Design Serious Cyber Games

This questionnaire is to collect your impressions about the proposed pedagogical design model MOTENS for serious cyber games. The answers to this questionnaire are NOT used by any means to evaluate/grade you, and your responses will not be attributed to you as an anonymous questionnaire.

The questions are based on the Technology Acceptance Model (TAM): Perceived Ease of Use (PEOU), Perceived Usefulness (PU) and Intention to Use (ITU).

This questionnaire should only take you 15 minutes to complete. Please look at each model and answer the following questions:

		Model 1: LM-GM Model Scores					Model 2: MOTENS Model Scores				
No	**Question**	**Strongly Disagree 1**	**Disagree 2**	**Neutral 3**	**Agree 4**	**Strongly Agree 5**	**Strongly Disagree 1**	**Disagree 2**	**Neutral 3**	**Agree 4**	**Strongly Agree 5**
Section 1 – Perceived Usefulness (PU)											
1	It will be useful to use the model to help designing serious cyber games that are effective for players to learn desired cyber educational objectives.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Section 2 – Perceived Ease of Use (PEOU)											
2	Using the model to design serious cyber games, I can see it will be easy to map gameplay to the game mechanics and support the pedagogical educational theory and learning, not just creating a fun game to play.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Section 3 – Intension to Use (ITU)											
3	Overall, I think the model will help design serious cyber games to meet intended learning objectives and educational effectiveness. I would use it or recommend using it to help design serious cyber games.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

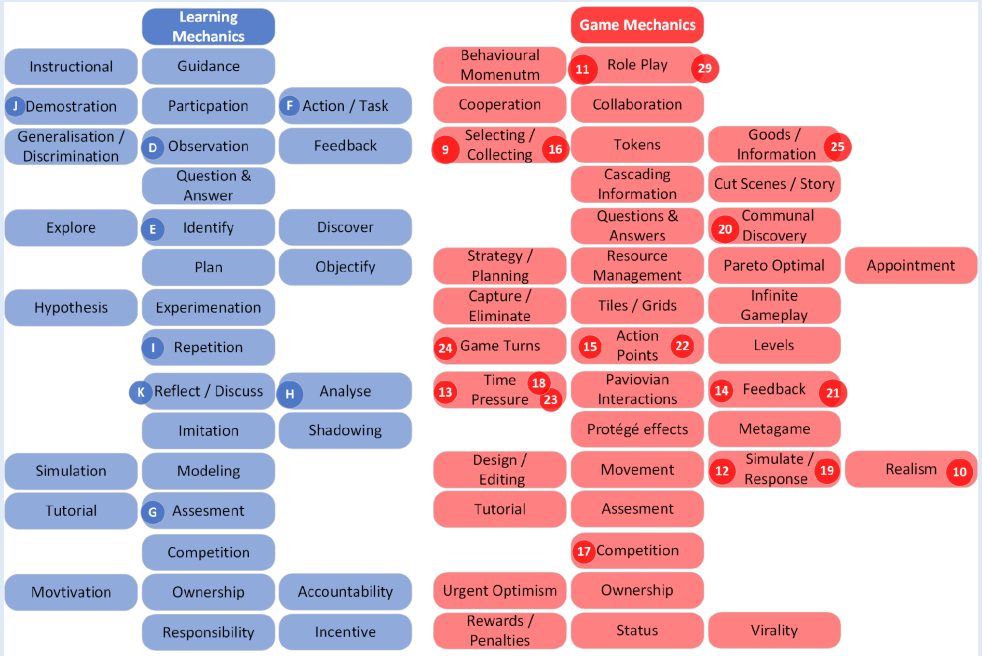
Please email completed forms to research student: Mr Stephen Hart

Email: stephen.hart@soton.ac.uk **University of Southampton:** https://www.ecs.soton.ac.uk/people/sjh1n15 **Riskio Website:** https://www.riskio.co.uk

Privacy Statement: No personal data will be collected, and your participation will be confidential.

Figure K.1: MOTENS Case Study - Page 1: Questionnaire.

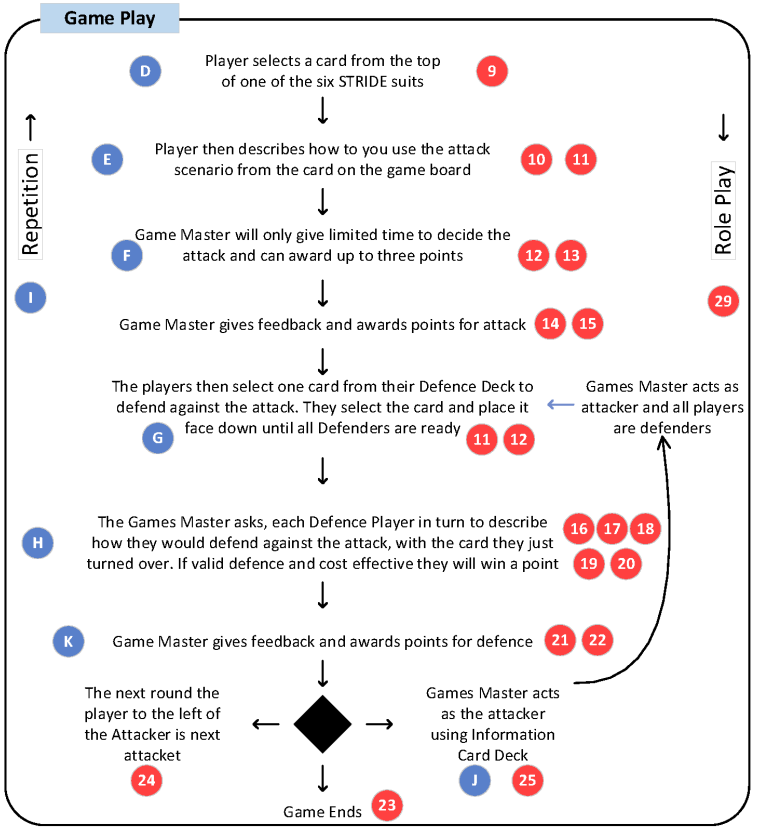
Model 1 - LM-GM Model



Note:

1. Numbers and letters added to the model to map to the game, not on the original LM-GM model

LM-GM Model – Mapping Learning Mechanics to Game Mechanics



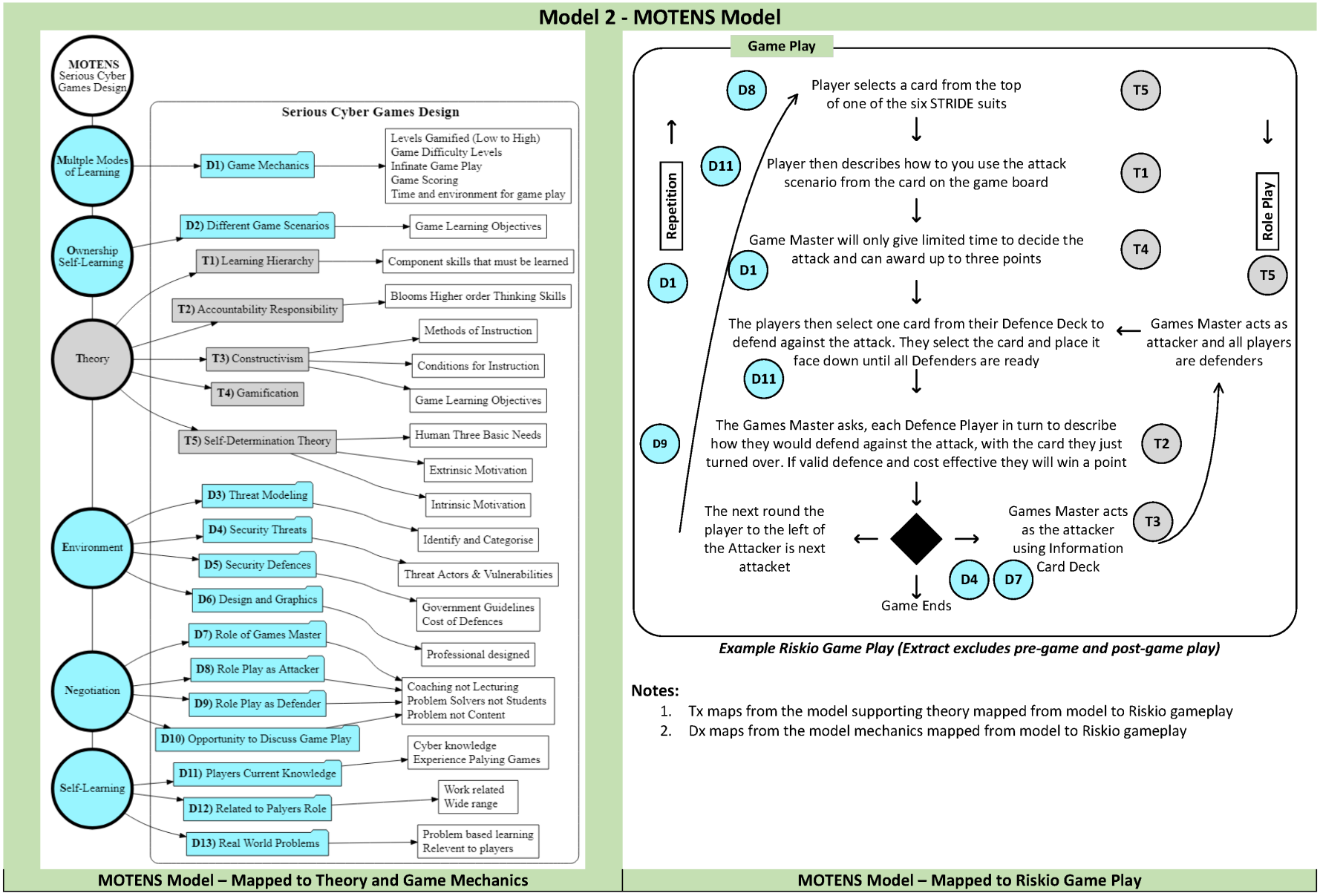
Example Riskio Game Play (Extract excludes pre-game and post-game play)

Notes:

1. The numbering maps Game Mechanics from model to Riskio gameplay
2. The letters map Learning Mechanics from model to Riskio gameplay

LM-GM Model – Mapped to Riskio Game Play

Figure K.2: MOTENS Case Study - Page 2: Riskio mapped to LM-GM Model.



Example Riskio Game Play (Extract excludes pre-game and post-game play)

Notes:

1. Tx maps from the model supporting theory mapped from model to Riskio gameplay
2. Dx maps from the model mechanics mapped from model to Riskio gameplay

Figure K.3: MOTENS Case Study - Page 3: Riskio mapped to MOTENS Model.

Appendix L

CIST Game Questionnaire

This questionnaire collects your impressions about the CIST Threat Model & Serious single-player Game to teach threats, vulnerabilities, and countermeasures to the IC Supply Chain. The answers to this questionnaire are NOT used by any means to evaluate/grade you. The first part of this questionnaire is background information, and please do not enter any personal information. The second part of this questionnaire is in four sections and are based on the Technology Acceptance Model (TAM): Perceived Ease of Use (PEOU), Perceived Usefulness (PU) and Intention to Use (ITU).

Section 1

1. Which team/function area do you work in at your organisation?
☐ Working for a University as Professor; Associate Professor or Lecturer
☐ Working for a University in the Research Department
☐ Working for UK Government in the Research Department
☐ Working for Organisation in the Research Department
☐ PhD Student
☐ MSc/BSc Student
☐ Other Please state _____

2. How would you describe your level of expertise in threats to IC supply chain?
Please choose only one of the following options:
novice ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 expert

3. How would you describe your level of expertise in Hardware security awareness and education?
Please choose only one of the following options:
novice ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 expert

Read each question carefully as each question can be positive or negative.

If you strongly disagree with the statement, check the leftmost box (1).
If you disagree, with the statement, check box #2 from the left (2).
If you agree with neither statement, check the middle box (3).
If you agree, with the statement, check box #4 from the right (4).
If you agree strongly with the statement, check the rightmost box (5).

Table L.1: CIST Post-Game Questionnaire.

No	Question	Strongly Disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly Agree 5
	Section 1 – Perceived Relevance to IC Supply Chain (PU)					
	Learning Features					
1	Control - Players in control and can learn at their own pace.	☐	☐	☐	☐	☐
2	Challenge – The game provides sufficient to challenge the players.	☐	☐	☐	☐	☐
3	Feedback – Players know how to improve their answers through game feedback.	☐	☐	☐	☐	☐
	Learning Outcomes					
4	Threats – Players will be able to identify key threats and location in the IC supply chain.	☐	☐	☐	☐	☐
5	Countermeasures – Players will be able to identify defence as a countermeasure to threats.	☐	☐	☐	☐	☐
6	Autodidact – Players more likely to take control of self-learning over presenting the same 30 attacks in traditional classroom presentation.	☐	☐	☐	☐	☐

Continued on next page

Table L.1 – continued from previous page

	Section 2 - Perceived Ease of Use (PEOU)					
7	I feel that players would want to play this game to increase knowledge in risk management of the IC supply chain.	☐	☐	☐	☐	☐
8	I feel playing the CIST game will be easy for the player to learn about a given attack about adversaries able to complete the attack and location and potential countermeasures.	☐	☐	☐	☐	☐
	Section 3 - Intention to Use (ITU)					
9	Overall, I would recommend using the CIST game to learn about hardware vulnerabilities in the IC. Supply chain and countermeasures.	☐	☐	☐	☐	☐
	Please enter any additional comments					

Participant Information - What is the research about?

The research is for my PhD, and the main aim of the research is to educate employees on the nature of the risks coming from cyber attacks and the best strategies to defend against them. I have created a pedagogical model called MOTENS to support the design of serious cyber games for awareness and education. The CIST game was designed using the MOTENS model, and the CIST game was created to verify the MOTENS model. If you require any additional information, please see the contact information below:

Contact for research student: Mr Stephen Hart

Email: stephen.hart@soton.ac.uk
University of Southampton: www.ecs.soton.ac.uk/people/sjh1n15
CIST Game: https://mygame.page/cist-game/
Previous game created: https://www.riskio.co.uk/

Privacy Statement

Your participation will be confidential, and no personal data will be collected. If any participant mentions something in comments section which could identify an individual this will not be used in the research and where feasible this will be securely destroyed.

Appendix M

CIST Game Design

CIST Game Design Using MOTENS Model

This section creates the CIST game: A Serious Game for Hardware Security Supply Chain designed using the MOTENS Model from Chapter 7.

MOTENS Design Stages The game will be created by going through the MOTENS five design stages (see subsection 7.3.1). The MOTENS five design stages, however, can be iterative.

Stage 1: Target Players (Segmentation). The primary target for the game will be university students working in electronics and computer science, including cyber and information security. The students have been identified as gamers and require high gamified content. We also identified a secondary audience as new employees working in the IC hardware supply chain can also play the game. In the secondary group, employees come from a broader range of backgrounds and might not have the same level of technical knowledge as students.

Stage 2: Type of Game. We want to create a game for a secure IC hardware supply chain for security awareness and education of the threats and possible countermeasures in the IC hardware supply chain. The game will be an online single-player game, and the game does not require a games master.

Stage 3: MOTENS Design Initial Map. This stage creates the initial design map using the MOTENS model, see Figure 7.6. The initial mapping noted potential differences in requirements for **D1)** Game Mechanics and **D4)** Security Threats see Figure M.1.

Stage 4: Design Gameplay/Mechanics. The first step is to map the potential gameplay design elements and consider any potential differences found in stage 3 and the initial design map see Figure M.1. In the creation of this map of gameplay mapped to the MOTENS model, see Figure M.2.

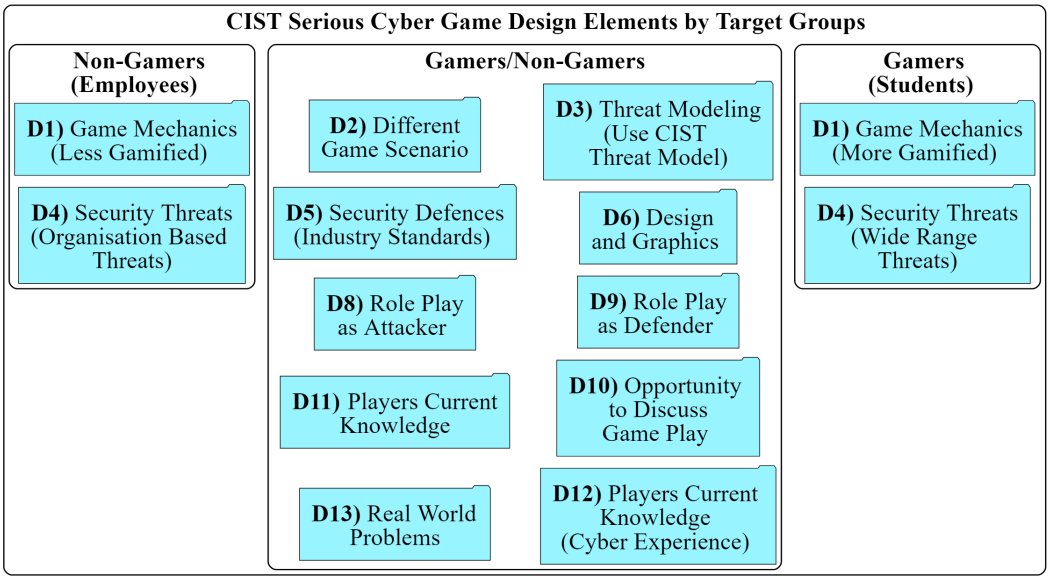


Figure M.1: MOTENS Design Stage 3: CIST Initial Design Map.

Step 1: Game Design - Initial Decisions (T1) & (T4)

(a) Use the CIST threat model to categorise the threats as designed for hardware threats (D3)
(b) Use most common current industry defences for the game by CIST category (D5)
(c) Design/Graphics: use icons to represent, Adversaries, Attack Location, Defences and Information (D6), see Figure M.3 & M.4
(d) Select most common hardware threats for the attacks (D4, D12)
(e) Threats about real-world problems to target players (D13)
(f) Can change the database of threats to increase game difficulty (D1) and game scenarios (D2)

Step 2: Pre-Gameplay (T3), & (T4)

(a) A brief presentation on the CIST threat model (D3)
(b) A brief explanation of the most common threats to the hardware supply chain (D2 D11), see Figure M.5 & M.6
(c) Numbered step by step guide on how players select options to defend from attack (D8)

Step 3: Gameplay (T1), (T2), (T3), (T4), & (T5)

(a) Allow players to select threat category, adversary, location of attack and defence in any order (D9)
(b) Mark all attacks with a unique ID for players to give feedback (D10)
(c) The player has the opportunity to play the role of attacker, must be able to identify the capability of adversaries and location in the IC supply chain where they can attack (D8)
(d) The player has the opportunity to play the role of defender, must be able to select countermeasures to the attacks (D9)

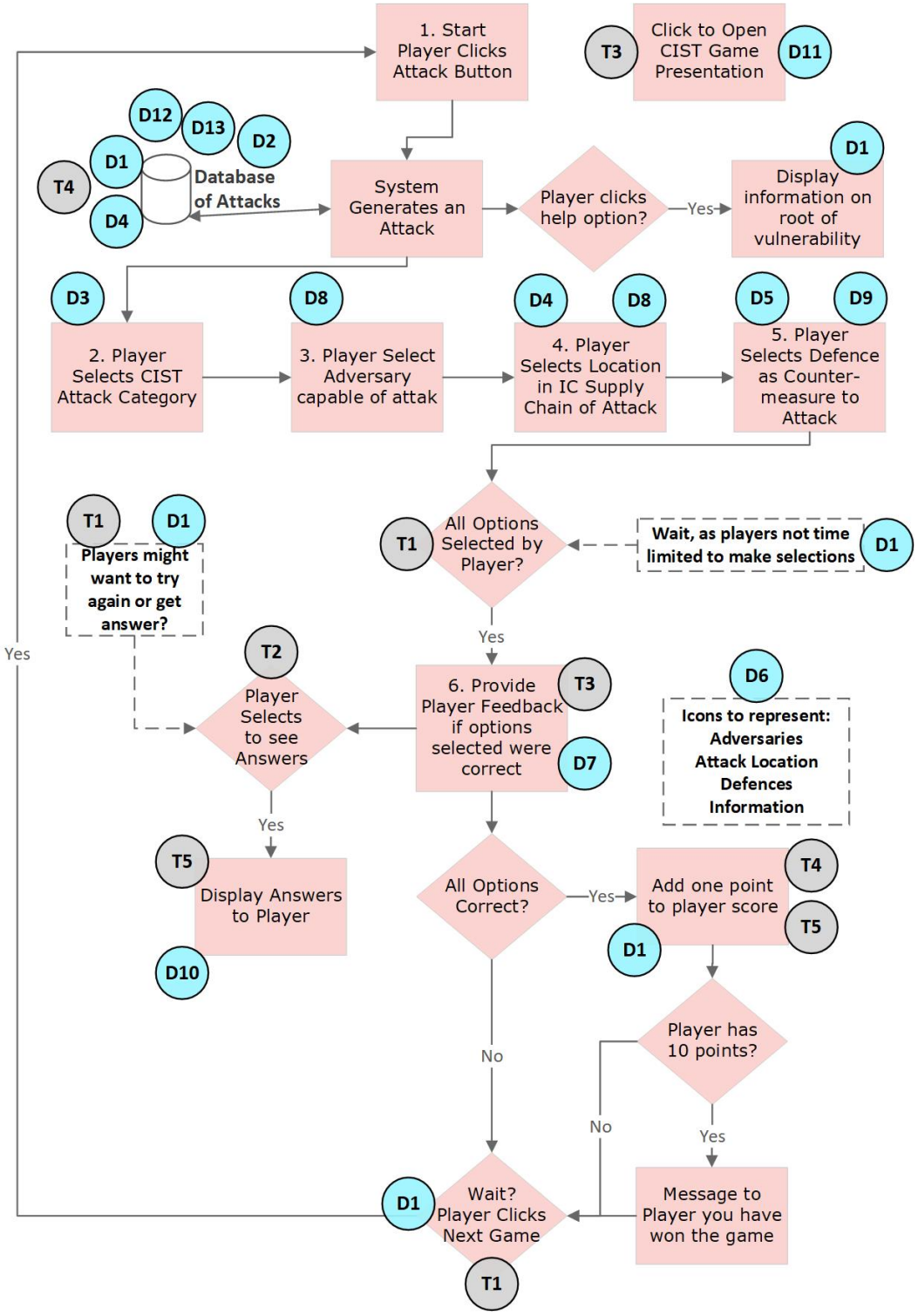


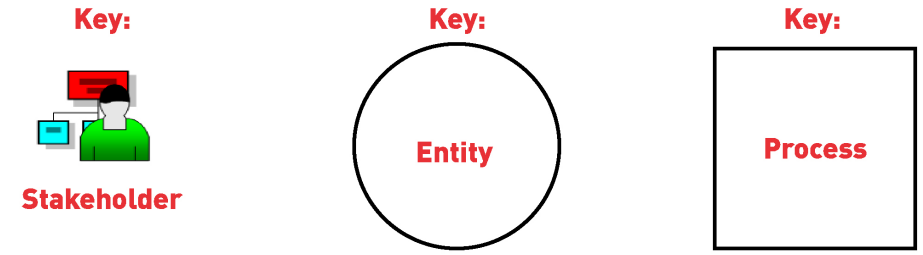
Figure M.2: CIST Gameplay Mapped to MOTENS Model.

(e) Target players students with a technical background but might not be aware of specific hardware threats, display information on root of vulnerability (D1)

(f) Players might not understand some of the terms used in the IC hardware supply chain, and if a user clicks on any tile, they flip over to reveal more information. Information

(a) Adversaries Icon (b) Attack Icon (c) Defence Icon (d) Information Icon

Figure M.3: CIST Game Icons.



(a) Stakeholder Key (b) Entity Key (c) Process Key

Figure M.4: CIST Game Key Map.

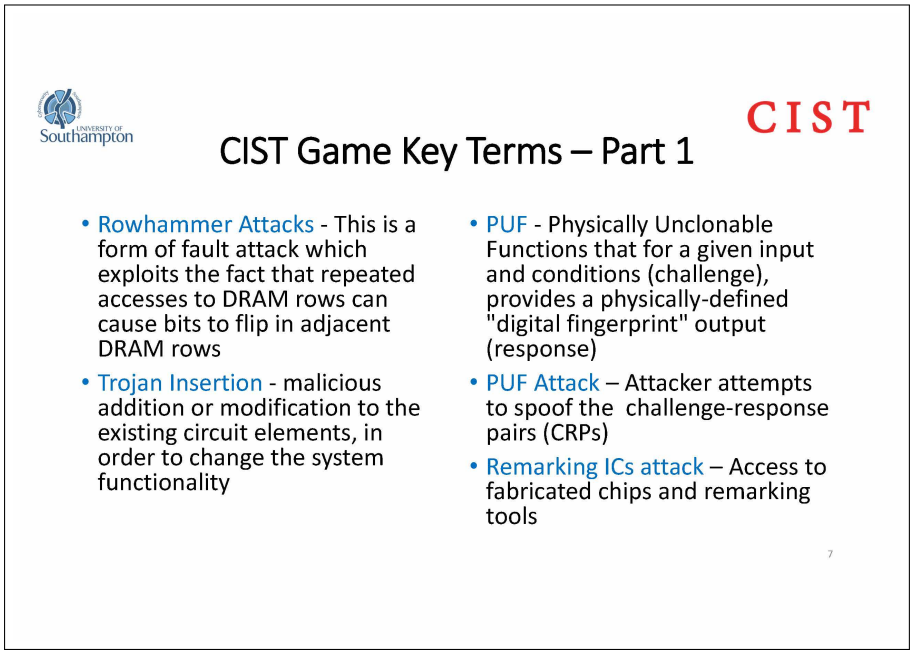


Figure M.5: CIST Game Tutorial - Slide 7.

about CIST Categories, see Figure M.7 and information about IC hardware supply chain, see Figure M.8

(g) Players can click on the information card to find the root of the vulnerability, see Figure M.9

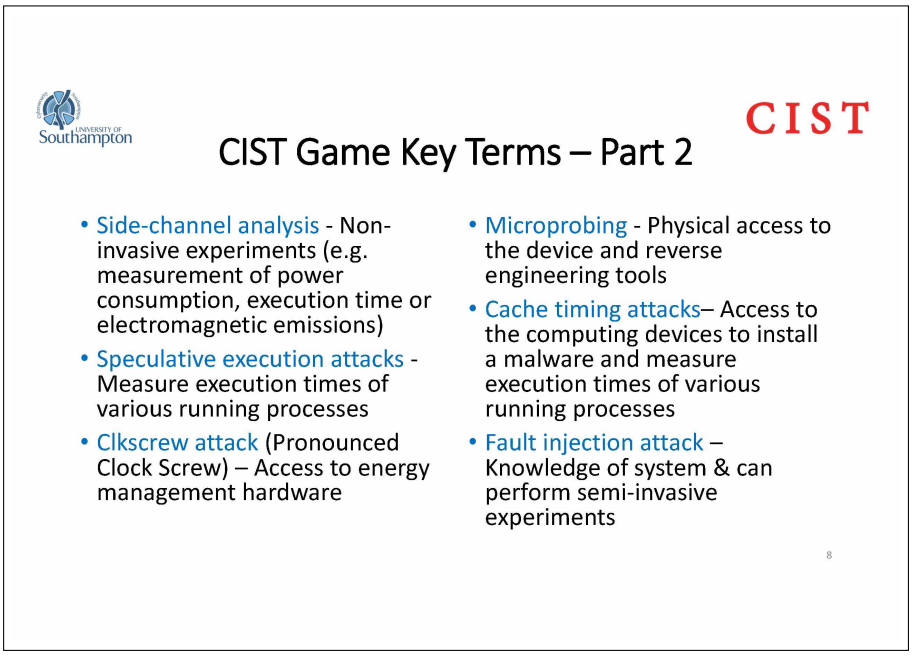


Figure M.6: CIST Game Tutorial - Slide 8.

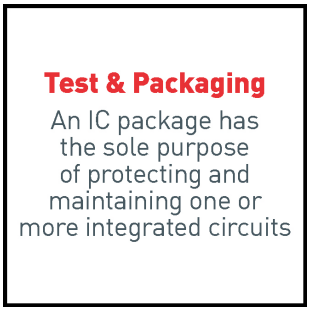
(a) Counterfeiting Tile Front

(b) Counterfeiting Tile Back

Figure M.7: CIST Game Tiles Front and Back of Counterfeiting Tile.

(a) Stakeholder Example

(b) Entity Example

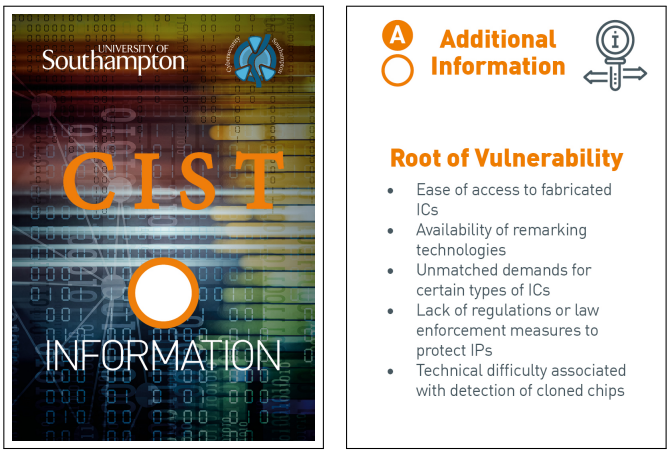


(c) Process Example

Figure M.8: CIST Game Tiles Back of Tile Examples.

Step 4: Game End (T2), & (T3)

(a) Feedback to players if each answer on threat category, adversary, location and defence were correct. (D10)



(a) Back Information (b) Information For Player

Figure M.9: CIST Game Information Root of Vulnerability Attack ID: 15.

(b) Link to answer after completed defence as the game does not have games master so the player can learn from mistakes (D7 & D11)

Step 5: Review and Test Design

(a) Feedback was difficult for test players, so a unique ID was added for every attack to assist

(b) The game was initially deployed as Windows standalone executable application, and users were concerned about getting a security warning or had other operating systems unable to run the program. The game was then deployed as an online game

Stage 5: Design Test and Evaluate Feedback: Why not highlight the six steps to each game round? The decision to allow players to select an option in any order was deliberate in the design as felt gamers would like to select the options in any order, for example, Adversary then CIST category rather than forcing players to select CIST category first. Enforcing the order, the player selects options requires further testing in stage 5. See Figure M.10 for an example of the game board.

Example CIST Gameplay & How code to attacks This section explains the CIST gameplay with one example.

Example CIST Gameplay The gameplay for the CIST game is in six steps. This section goes through the six steps of gameplay.

Start Player before starting can select the option to see a tutorial presentation on the game and information about the CIST threat model includes top threats to IC hardware supply chain

Step 1 Player clicks on a button to generate an attack. See Figure M.11 (Note each attack has a unique attack ID)

Step 2 Read the attack and select the correct CIST threat category by clicking on the tile to turn over, see Figure M.12 feedback on selected option

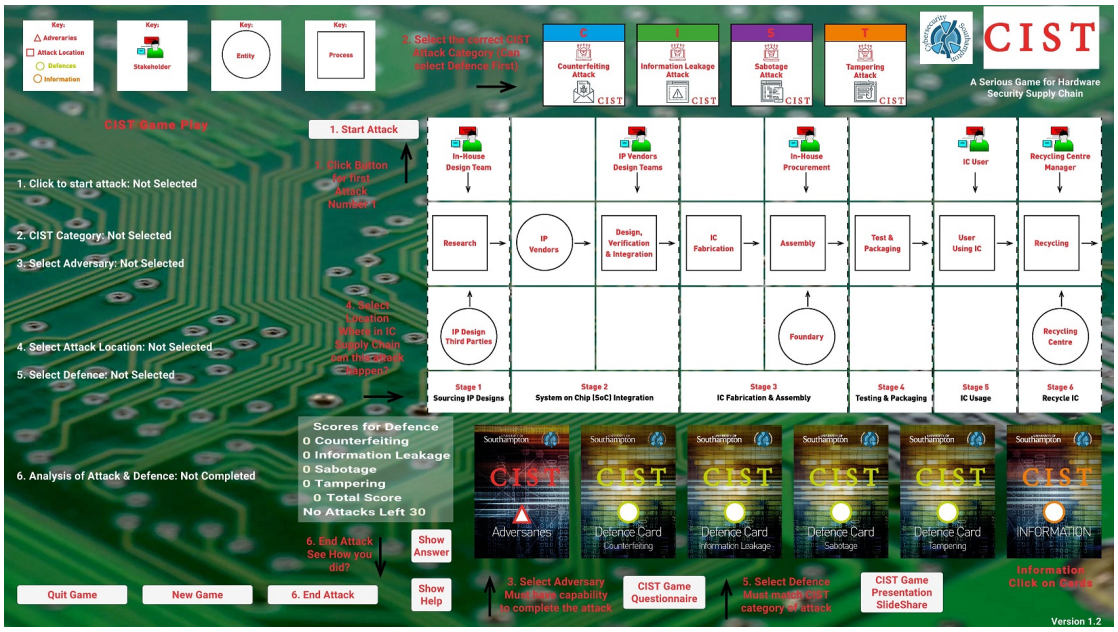


Figure M.10: CIST Game Screen Shot.

Figure M.11: CIST Gameplay Player Clicks Start Attack.

Figure M.12: CIST Game Player selects CIST Threat Category.

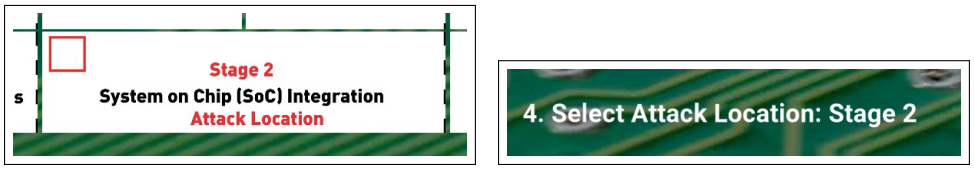
Step 3 Player clicks on adversary deck of cards to select an adversary capable of the attack, see Figure M.13, see Figure M.14 feedback on selected option

(a) Adversaries Class 1 (b) Adversaries Class 2 (c) Adversaries Class 3 (d) Adversaries Class 4

Figure M.13: CIST Game Adversaries: Class 1 to Class 4.

Figure M.14: CIST Game Player selects adversary capable of attack.

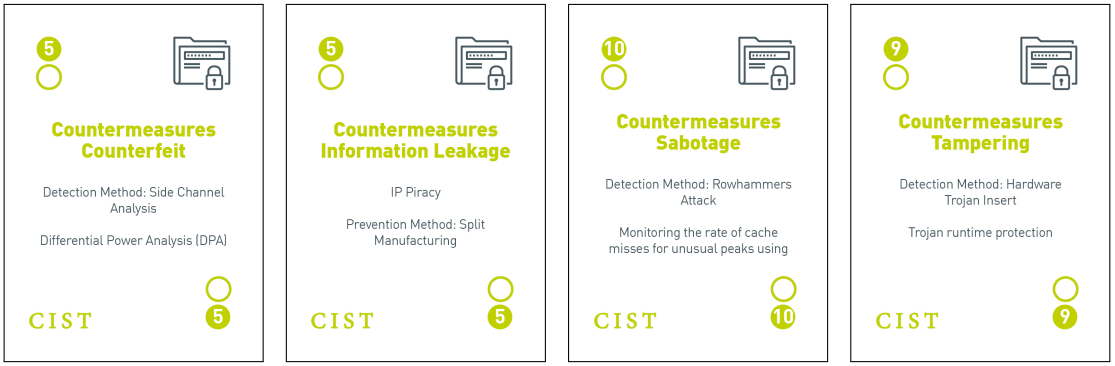
Step 4 Player clicks on stage location where they think attack can happen, the stage user selects places red square at location (see item M.15(a)) and changes the text in feedback area of the game (see item M.15(b))



(a) Feedback from Stage Clicked (b) Feedback Player Selected Option

Figure M.15: CIST Game Example Selecting Location (Stage) of Attack

Step 5 Player selects the countermeasure to the attack based on CIST category and location of attack could require different defence, see Figure M.16 and see Figure M.17 feedback on selected option



(a) Counterfeiting (b) Information Leakage (c) Sabotage (d) Tampering

Figure M.16: CIST Game Defence Example Cards.

Figure M.17: CIST Gameplay Player Selects Defence.

Step 6 After the player has finished selecting all options, and they can then click to end the attack and get an analysis of the options they selected, see Figure M.18

Codified CIST Game Attack Figure M.19 is an example of an attack for the CIST game. Attack ID No: 15 (unique ID); Sequence: 28 (the number order for this attack); CIST Category:

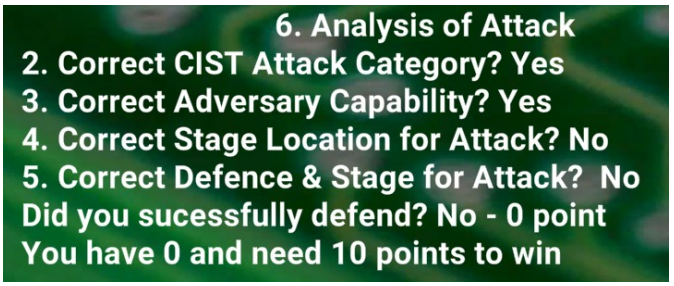


Figure M.18: CIST Game End Attack Analysis - Feedback to Player.

Counterfeiting (for this attack); Min Attack Level: 2 (Level capability of attacker required); Stage Attack Possible (Boolean value for all the stages); Defences: for each stage where the attack is possible, the list of defence IDS possible for the countermeasure to the attack; and Help: 'Description of the Root of Vulnerability of Attack, to help the player', only displayed if you select this option. The codification of attacks enables creating a database of attacks to be extended or changed based on players or game scenarios.

Attack ID No	Sequence	Description of Attack
15	28	An attacker has access to a fabricated chips and IC remarking tool to remark ICs

CIST Category	Counterfeiting	Information Leakage	Sabotage	Tampering
	True	False	False	False
Attacker	Class 1 - Adversary A small group of curious hackers Attack Level can wage 1-2	Class 2 - Adversary An academic research group Attack Level can wage 1-3	Class 3 - Adversary An organised criminal gang Attack Level can wage 1-3	Class 4 - Adversary A state-funded Organisation Attack Level can wage 1-4
Highest Level	2	3	3	4
Min Attack Level	2			

Stages	Stage 1 Sourcing IP Designs	Stage 2 System on Chip (SoC) Integration	Stage 3 IC Fabrication & Assembly	Stage 4 Testing & Packaging	Stage 5 IC Usage	Stage 6 Recycling IC
Stage Attack Possible?			Yes	Yes	Yes	Yes

Defences ID No	Counterfeiting Defence IDs			Information Leakage Defence IDs			Sabotage Defence IDs			Tampering Defence IDs		
Stage 1	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 2	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 3	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 4	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 5	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						
Stage 6	1	2	3	10	11	12	19	20	21	23	24	25
	4	5	6	13	14	15	22			26	27	
	7	8	9	16	17	18						

Help	Description
	Root of vulnerability • Ease of access to fabricated ICs • Availability of remarking technologies • Unmatched demands for certain types of ICs • Lack of regulations or law enforcement measures to protect IPs • Technical difficulty associated with detection of cloned chips

Defence ID (Card)	Defence
3 (7)	Detection Method: Fingerprinting Conventional serial numbers
4 (8)	Detection Method: Fingerprinting DNA Marking
6 (10)	Detection Method: Fingerprinting: Digital Fingerprinting

Figure M.19: CIST Game Example of Attack.

Appendix N

Riskio Game ERGO 44919 Ethics Application

Status: Approved

The end date for this study was the 30th of September 2019. This ethical approval covers the four experiments described in Section 4.1 game development and Section 5.2 study realisation. The four experiments dates:

Experiment 1	October 2018 - Member of Cyber Security Academy (CSA) 14 graduate students
Experiment 2	October 2018 - Secure Software Development Course 15 students enrolled in the MSc in Cyber Security and Software Engineering
Experiment 3	January 2019 - Professional training course on "Cyber security awareness" 12 employees
Experiment 4	April 2019 - Part of a professional training course for "Chief Data Officers" 13 legal practitioners

FPSE Ethics Committee
FPSE EC Application Form **Ver 6.6e**

Reference number: **ERGO**/FPSE/**44919**	Submission version: 1	Date: 28-07-2018
Name of investigator(s): **Mr Stephen Hart**		
Name of supervisor(s) (if student investigator(s)): **Dr Federica Paci** **Professor Vladimiro Sassone**		
Title of study: **A card game to raise awareness of cyber security to identify threats and possible defences**		
Expected study start date: 18/09/2018	Expected study end date: 19/09/2018	

Note that the dates requested on the "IRGA" form refer to the start and end of data collection. These are not the same as the start and end dates of the study, above, for which approval is sought. (A study may be considered to end when its final report is submitted.)
Note that ethics approval must be obtained before the expected study start date as given above; retrospective approval cannot be given.
Note that failure to follow the University's policy on Ethics may lead to disciplinary action concerning Misconduct or a breach of Academic Integrity.
By submitting this application, the investigator(s) undertake to:

- Conduct the study in accordance with University policies governing:
  Ethics (http://www.southampton.ac.uk/ris/policies/ethics.html);
  Data management (http://www.southampton.ac.uk/library/research/researchdata/);
  Health and Safety (http://www.southampton.ac.uk/healthandsafety);
  Academic Integrity (http://www.calendar.soton.ac.uk/sectionIV/academic-integrity-statement.html.
- Ensure the study Reference number ERGO/FPSE/44919 is prominently displayed on all advertising and study materials, and is reported on all media and in all publications;
- Conduct the study in accordance with the information provided in the application, its appendices, and any other documents submitted;
- Submit the study for re-review (as an amendment through ERGO) or seek FPSE EC advice if any changes, circumstances, or outcomes materially affect the study or the information given;
- Promptly advise an appropriate authority (Research Governance Office) of any adverse study outcomes (via an adverse event notification through ERGO);
- Submit an end-of-study form if required to do so.

REFER TO THE INSTRUCTIONS AND GUIDE DOCUMENTS WHEN COMPLETING THIS FORM AND THE TEMPLATES DOCUMENT WHEN PREPARING THE REQUIRED APPENDICES.

Pre-STUDY

Characterise the proposed participants
The participants will be attending a continued professional development (CPD) course run by Southampton University Cyber Security Academy from 18th to the 19th September 2018.

Describe how participants will be approached
The participants will be approached at the start of the CPD course and the background explained using the participant information sheet.

Describe how inclusion and/or exclusion criteria will be applied (if any)
There are 20 potential participants attending the CPD course. The game will be played in group of 5 participants. The groups will be re-organised if some attendees decide to opt out of the research.

Describe how participants will decide whether to take part
The participants will be asked to sign the consent form. If they do not want to take part to the study, the subjects can play the game as part of Cyber CPD course but no data will be collected from them.

Participant Information (Appendix (i))

Provide the Participant Information in the form that it will be given to participants as Appendix (i). All studies must provide participant information.

Consent Form/Information (Appendix (iii))

Provide the Consent Form (or the request for consent) in the form that it will be given to participants as Appendix (iii). All studies must obtain participant consent. Some studies may obtain verbal consent (and only present consent information), other studies will require written consent, as explained in the Instructions, Guide, and Templates documents.

FPSE EC Application Form

DURING THE STUDY

Describe the study procedures as they will be experienced by the participant
The study will start by explaining to the participants the general purpose of the study and introducing the game to the participants. Then the participants will be asked to fill in the consent form and if they agree to participate to the study, they will be asked to fill the background and security awareness questionnaire. Then the participants will be divided in group of 5 and they will start playing the game under the direction of the Games Master. Each team requires a deck of Attack Cards. Each player in the team needs a deck of Defence Cards. One player acts as the attacker and the others act as the defenders and then take turns to act as the attacker. The attacker player can get up to three points for a valid attack and the defence players can get up to three points for defending against the attack. Games master sometimes in bonus round acts as the attacker and players can win up to three points for valid defence. The game is played in rounds with points awarded in each round. At the end of the game the participants will be asked to fill in the game assessment questionnaire.

Identify how, when, where, and what kind of data will be recorded (not just the formal research data, but including all other study data such as e-mail addresses and signed consent forms)
Before the game starts: * Participants consent form * Participants background and security awareness questionnaire **During the game play. The following data will be written down for each round:** * The card the attacker played (Attack card deck six suits in 2 to 10, Jack, Queen and Ace) * The cards the defenders played (Defence card deck one suits in 2 to 10, Jack, Queen and Ace) * The card played if the Games Master played an Information Card as a Bonus (Information card deck one suits in 2 to 10, Jack, Queen and Ace) * Points awarded to the players * Comments on the game play made by the players. We will not record which player said the comments or anything that could identify a data subject. **After the game: Game Assessment Questionnaire**

Participant questionnaire/data gathering methods (Appendix (ii))

As Appendix (ii), reproduce any and all participant questionnaires or data gathering instruments in the exact forms that they will be given to or experienced by participants. If conducting less formal data collection, or data collection that does not involve direct questioning or observation of participants (e.g. secondary data or "big data"), provide specific information concerning the methods that will be used to obtain the data of the study.

POST STUDY

Identify how, when, and where data will be stored, processed, and destroyed
Data will be stored on encrypted on the Investigator's laptop. The data will be held in accordance with University policy on data retention. Data files will be protected by encryption; laptops will be protected by access control using strong password and have updated anti-virus software installed; desktops will be protected by using Southampton University managed devices; physical data will be kept in filing cabinets and protected by locks on the cabinets. The physical data will be destroyed using secure shredding bins at Southampton University. Electronic data will be deleted and where possible backup copies and recycle bin the data will also be deleted. The data will be processed in accordance with the rights of the participants because they will have the right to access, correct, and/or withdraw their data at any time and for any reason. Participants will be able to exercise their rights by contacting the investigator (e-mail: sjh1n15@ecs.soton.ac.uk) or the project supervisor (e-mail: F.M.Paci@soton.ac.uk). The data will be anonymised by using random 4-digit number and the Consent forms will not be linked to the data by the use of the random 4-digit number. However, the questionnaire before the game and after the game will be linked by the 4-digit number. The processing of the data does not require identification of the data subject (Article 11 GDPR), however the data subject will have given the right to be forgotten and stop further processing by remembering their anonymised number they can use this random 4-digit number later and request that data linked to them to be removed from further processing and deleted. However, participants are asked to confirm in the consent form "I understand that if I withdraw my consent later after the anonymised data has been published it will be impossible to have this deleted." No data will be transferred outside the European Economic Area (EEA).

STUDY CHARACTERISTICS

(L.1) The study is funded by a commercial organisation: **No** (delete one) If 'Yes', provide details of the funder or funding agency here.

(L.2) There are restrictions upon the study: **No** (delete one) If 'Yes', explain the nature and necessity of the restrictions here.

FPSE EC Application Form

(L.3) Access to participants is through a third party: **No** (delete one)
If 'Yes', provide evidence of your permission to contact them as Appendix (v). Do not provide explanation or information on this matter here.

(M.1) Personal data is or *may be collected or processed: **Yes** (delete one) Data will be processed outside the UK: No (delete one) If 'Yes' to either question, provide the DPA Plan as Appendix (iv). Do not provide information or explanation on this matter here. Note that using or recording e-mail addresses, telephone numbers, signed consent forms, or similar study-related personal data requires M.1 to be "Yes". (* Secondary data / "big data" may be de-anonymised, or may contain personal data. If so, answer 'Yes'.)

(M.2) There is inducement to participants: **No** (delete one) If 'Yes', explain the nature and necessity of the inducement here.

(M.3) The study is intrusive: **No** (delete one) If 'Yes', provide the Risk Management Plan, the Debrief Plan, and Technical Details as Appendices (vi), (vii), and (ix), and explain here the nature and necessity of the intrusion(s).

(M.4) There is risk of harm during the study: **No** (delete one) If 'Yes', provide the Risk Management Plan, the Contact Information, the Debrief Plan, and Technical Details as Appendices (vi), (vii), (viii), and (ix), and explain here the necessity of the risks.

(M.5) The true purpose of the study will be hidden from participants: **No** (delete one) The study involves deception of participants: **No** (delete one) If 'Yes' to either question, provide the Debrief Plan and Technical Details as Appendices (vii) and (ix), and explain here the necessity of the deception.

(M.6) Participants may be minors or otherwise have diminished capacity: **No** (delete one) If 'Yes', AND if one or more Study Characteristics in categories M or H applies, provide the Risk Management Plan, the Contact Information, and Technical Details as Appendices (vi), (vii), & (ix), and explain here the special arrangements that will ensure informed consent.

(M.7) Sensitive data is collected or processed: **No** (delete one) If 'Yes', provide the DPA Plan and Technical Details as Appendices (iv) and (ix). Do not provide explanation or information on this matter here.

(H.1) The study involves: invasive equipment, material(s), or process(es); or participants who are not able to withdraw at any time and for any reason; or animals; or human tissue; or biological samples: **No** (delete one) If 'Yes', provide Technical Details and further justifications as Appendices (ix) and (x). Do not provide explanation or information on these matters here. Note that the study will require separate approval by the Research Governance Office.

Technical details
If one or more Study Characteristics in categories M.3 to M.7 or H applies, provide the description of the technical details of the experimental or study design, the power calculation(s) which yield the required sample size(s), and how the data will be analysed, as separate appendices.

APPENDICES (AS REQUIRED)

While it is preferred that this information is included here in the application form, it may be provided as separate document files. If provided separately, name the files precisely as "Participant Information", "Questionnaire", "Consent Form", "DPA Plan", "Permission to contact", "Risk Management Plan", "Debrief Plan", "Contact Information", and/or "Technical details" as appropriate. Each appendix or document must specify the reference number in the form ERGO/FPSE/xxxx, the document version number, and its date of last edit.

Appendix (i): **Participant Information** in the form that it will be given to **participants**.
Appendix (ii): Data collection method (e.g. for secondary data or "big data") **/ Participant** Questionnaire in the form that it will be given to **participants**.
Appendix (iii): **Consent Form** (or consent information if no personal data is collected) in the form that it will be given to participants.
Appendix (iv): **DPA Plan**.
Appendix (v): Evidence of permission to contact (prospective) participants through any third party.
Appendix (vi): **Risk Management Plan**.
Appendix (vii): **Debrief Plan**.
Appendix (viii): **Contact Information**.
Appendix (ix): Technical details of the experimental or study design, the power calculation(s) for the required sample size(s), and how the data will be analysed.
Appendix (x): Further details and justifications in the case of: **invasive** equipment, material(s), or process(es); **participants** who are not able to withdraw at any time and for any reason; animals; human tissue; or biological samples.

Appendix O

Data Protection Plan - ERGO 44919 Ethics Application

The following is the data protection plan for the four Riskio experiments (see Appendix N).

ERGO 44919 **Data Protection Plan**

Ethics reference number: **ERGO**/FPSE/**44919**	Version: 1.1	Date: 21-07-2018
Study Title: **A card game to raise awareness of cyber security to identify threats and possible defences.**		
Investigator: **Mr Stephen Hart**		

The following is an exhaustive and complete list of all the data that will be collected (through questionnaires, interviews, extraction from records, etc.)

- Questionnaire 1 Participants Background and Security Awareness – Used before game play (see attached, 10 questions)
    1. Role in organisation;
    2. Highest level of education;
    3. What degree you have;
    4. Level expertise in cyber security;
    5. level expertise in current attack trends;
    6. Qualifications in Cyber Security;
    7. Expertise in Information Technology;
    8. Expertise in Physical building security;
    9. Expertise in Risk assessments;
    10. Expertise in Microsoft STRIDE
- Questionnaire 2 Riskio Game Assessment – Used after game play (see attached 16 questions)

  The questions are regarding opinion of the game they played and opinion on how games can help to identify threats and improve cyber security knowledge
- Names of participants
- Email address
- Contact numbers
- Game score sheet (linked player number and not linked to data subject)

  The card the attacker played (Attack card deck six suits in 2 to 10, Jack, Queen and Ace) The cards the defenders played (Defence card deck one suits in 2 to 10, Jack, Queen and Ace)

  The card played if the Games Master played an Information Card as a Bonus (Information card deck one suits in 2 to 10, Jack, Queen and Ace)

  Points awarded to the players

  Comments on the game play made by the players but will not record a note which player said the comments or anything that could identify a data subject

The data is relevant to the study purposes because the research needs to understand the education and experience of the game players. The data is adequate because it's sufficient to fulfil the purpose of the research, and the data is not excessive because the research applied data minimisation principle and only collecting data necessary for the research.

ERGO 44919 **Data Protection Plan**

The data will be processed fairly because the results of the published data will be impossible to link back to a data subject. The participants will have given explicit consent through signing consent form which clearly states the data is anonymised in the research reports.

The data's accuracy is ensured because the data can't be linked to a data subject so the data subject right to rectification under GDPR Article 16 would not apply to the data collected in the questionnaires.

The data will be held in accordance with University policy on data retention.

Data files will be protected by encryption; laptops will be protected by access control using strong password and have updated anti-virus software installed; desktops will be protected by using Southampton University managed devices; physical data will be kept in filing cabinets and protected by locks on the cabinets.

The physical data will be destroyed using secure shredding bins at Southampton University. Electronic data will be deleted and where possible backup copies and recycle bin the data will also be deleted.

The data will be processed in accordance with the rights of the participants because they will have the right to access, correct, and/or withdraw their data at any time and for any reason. Participants will be able to exercise their rights by contacting the investigator (e-mail: *redacted*) or the project supervisor (e-mail: *redacted*).

The data will be anonymised by using random 4-digit number and the Consent forms will not be linked to the data using the random 4-digit number. However, the questionnaire before the game and after the game will be linked by the random 4-digit number.

The processing of the data does not require identification of the data subject (Article 11 GDPR), however the data subject will have given the right to be forgotten and stop further processing by remembering their anonymised number they can use this random 4-digit number later and request that data linked to them to be removed from further processing and deleted. However, participants are asked to confirm in the consent form "I understand that if I withdraw my consent later after the anonymised data has been published it will be impossible to have this deleted."

No data will be transferred outside the European Economic Area (EEA).

Appendix P

MOTENS ERGO 62140 Ethics Application

Status: Approved

The end date for this study was the 31st of August 2021. This ethical approval covers the experiments as described in Section 7.4 illustrative case study and Section 7.5 comparison case study.

UNIVERSITY OF Southampton

FEPS Ethics Committee
FEPS EC Application Form Ver 2

Reference number: **ERGO**/FEPS/**62140**	Submission version: 1	Date: 2020-12-03
Name of investigator(s): **Mr Stephen Hart**		
Name of supervisor(s) (if student investigator(s)): **Dr Basel Halak**		
Title of study: **MOTENS A pedagogical design model for design serious cyber games**		

Note that failure to follow the University's policy on Ethics may lead to disciplinary action concerning Misconduct or a breach of Academic Integrity.
By submitting this application, the investigator(s) undertake to:

- Conduct the study in accordance with University policies governing:
  Ethics (http://www.southampton.ac.uk/ris/policies/ethics.html);
  Data management (http://www.southampton.ac.uk/library/research/researchdata/);
  Health and Safety (http://www.southampton.ac.uk/healthandsafety);
  Academic Integrity (http://www.calendar.soton.ac.uk/sectionIV/academic-integrity-statement.html.
- Ensure the study Reference number ERGO/FEPS/44919 is prominently displayed on all advertising and study materials, and is reported on all media and in all publications;
- Conduct the study in accordance with the information provided in the application, its appendices, and any other documents submitted;
- Submit the study for re-review (as an amendment through ERGO) or seek FEPS EC advice if any changes, circumstances, or outcomes materially affect the study or the information given;
- Promptly advise an appropriate authority (Research Governance Office) of any adverse study outcomes (via an adverse event notification through ERGO);
- Submit an end-of-study form if required to do so.

REFER TO THE INSTRUCTIONS AND GUIDE DOCUMENTS WHEN COMPLETING THIS FORM AND THE TEMPLATES DOCUMENT WHEN PREPARING THE REQUIRED APPENDICES.

STUDY DETAILS

What are the aims and objectives of this study?
To evaluate a proposed design model called MOTENS that is used to design serious cyber games. The results of the study to be published in a scientific journal or conference paper.

Background of the study (a brief rationale for conducting the study)
This questionnaire is to collect impressions about the proposed pedagogical design model for serious cyber games called MOTENS. This is very targeted within cyber research community University, Government & private companies) that would use models to design serious cyber games. Riskio is a serious cyber game created by the application of a previous ERGO submission (Reference Number: ERGO/FEPS/44919) as part of previous research with University Southampton and is used to explain how the MOTENS model can be used to design serious games like Riskio.

Key research question (Specify hypothesis if applicable)
Is the proposed design model called MOTENS fill the current gaps in serious games design models and can be used to design serious cyber games.

Study design (Give a brief outline of the study design and why it is being used)
The design questionnaire is in two parts: The first part is about background of respondents (anonymised) and asks their previous knowledge of Riskio game used to explain the design model as Riskio has previously been presented within the cyber research community we need to verify no bias in results. The second part of the questionnaire study design uses the technology assessment model (TAM) to ask 8 questions to test the MOTENS model, perceived usefulness, perceived ease of use and intention to use.

Pre-STUDY

Characterise the proposed participants
The participants will be known to the researcher or supervisors, they will be working in area of cyber security research either: University as Professor; Associate Professor or Lecturer; University in the Research Department, for UK Government in the Research Department, Organisation in the Research Department or PhD student within Southampton University Cyber Security Academy.

Describe how participants will be approached
If any e-mail lists are used, including FEPS distribution lists, justify their use here They will be sent an email inviting them to take part no distribution lists will be used, or any emails collected from previous research. The participants are known to the research student or supervisors. The emails will be sent using blind copy (Bcc) or direct to the participant to ensure no email addresses are revealed to other recipients.

Describe how inclusion and/or exclusion criteria will be applied (if any)
No exclusion criteria will be applied but the inclusion is as follows: • Participants will be known to student researcher or supervisors • Participants may forward request to another person in the organisation working within cyber research area • Participants will all be working in the area of cyber security research or education and awareness

Describe how participants will decide whether to take part
If the participants decide to take part, they will be requested to email questionnaire back to the research student using Southampton University email address. Some participants may decide to email the supervisor via University email address, who will forward the email to the research student. It is also possible that some participants may return more than one completed questionnaire, this is acceptable as the questionnaires are anonymous and only need to verify the questionnaire came from a validated source.

Participant Information (Appendix (i))

Provide the Participant Information in the form that it will be given to participants as Appendix (i). All studies must provide participant information.

Consent Form/Information (Appendix (iii))

Provide the Consent Form (or the request for consent) in the form that it will be given to participants as Appendix (iii). All studies must obtain participant consent. Some studies may obtain verbal consent (and only present consent information), other studies will require written consent, as explained in the Instructions, Guide, and Templates documents.

DURING THE STUDY

Describe the study procedures as they will be experienced by the participant
The participant if external to the University of Southampton will receive an email with request to participate. The email will contain link to short (less than 10 minutes) video hosted on private link explaining the MOTENS model. The email will also have case study and other background information. The participant can then decide to complete the attached questionnaire (word version) they can return if they decide to take part or ignore the email and they will not be contacted.

Identify how, when, where, and what kind of data will be recorded (not just the formal research data, but including all other study data such as e-mail addresses and signed consent forms)
No personal data such as emails address etc. will be collected. Three background questions which cannot identify the participant and 10 questions on the MOTENS model using Likert scale. There is an area on the form titled "Please enter any additional comments further information.", if participants give identifiable information this will not be used in the researched. If the form needs to be shared internally within Southampton University, then if participant used identifiable information this will be redacted.

Participant questionnaire/data gathering methods (Appendix (ii))

As Appendix (ii), reproduce any and all participant questionnaires or data gathering instruments in the exact forms that they will be given to or experienced by participants. If conducting less formal data collection, or data collection that does not involve direct questioning or observation of participants (e.g. secondary data or "big data"), provide specific information concerning the methods that will be used to obtain the data of the study.

POST STUDY

Identify how, when, and where data will be stored, processed, and destroyed
Does not apply.

STUDY CHARACTERISTICS

(L.1) The study is funded by a commercial organisation: **No** (delete one) If 'Yes', provide details of the funder or funding agency here.

(L.2) There are restrictions upon the study: **No** (delete one) If 'Yes', explain the nature and necessity of the restrictions here.

(L.3) Access to participants is through a third party: **No** (delete one)
If 'Yes', provide evidence of your permission to contact them as Appendix (v). Do not provide explanation or information on this matter here.

(M.1) Personal data is or *may be collected or processed: **No** (delete one) Data will be processed outside the UK: No (delete one) If 'Yes' to either question, provide the DPA Plan as Appendix (iv). Do not provide information or explanation on this matter here. Note that using or recording e-mail addresses, telephone numbers, signed consent forms, or similar study-related personal data requires M.1 to be "Yes". (* Secondary data / "big data" may be de-anonymised, or may contain personal data. If so, answer 'Yes'.)

(M.2) There is inducement to participants: **No** (delete one) If 'Yes', explain the nature and necessity of the inducement here.

(M.3) The study is intrusive: **No** (delete one) If 'Yes', provide the Risk Management Plan, the Debrief Plan, and Technical Details as Appendices (vi), (vii), and (ix), and explain here the nature and necessity of the intrusion(s).

(M.4) There is risk of harm during the study: **No** (delete one) If 'Yes', provide the Risk Management Plan, the Contact Information, the Debrief Plan, and Technical Details as Appendices (vi), (vii), (viii), and (ix), and explain here the necessity of the risks.

(M.5) The true purpose of the study will be hidden from participants: **No** (delete one) The study involves deception of participants: **No** (delete one) If 'Yes' to either question, provide the Debrief Plan and Technical Details as Appendices (vii) and (ix), and explain here the necessity of the deception.

(M.6) Participants may be minors or otherwise have diminished capacity: **No** (delete one) If 'Yes', AND if one or more Study Characteristics in categories M or H applies, provide the Risk Management Plan, the Contact Information, and Technical Details as Appendices (vi), (vii), & (ix), and explain here the special arrangements that will ensure informed consent.

(M.7) Sensitive data is collected or processed: **No** (delete one) If 'Yes', provide the DPA Plan and Technical Details as Appendices (iv) and (ix). Do not provide explanation or information on this matter here.

(H.1) The study involves: invasive equipment, material(s), or process(es); or participants who are not able to withdraw at any time and for any reason; or animals; or human tissue; or biological samples: **No** (delete one) If 'Yes', provide Technical Details and further justifications as Appendices (ix) and (x). Do not provide explanation or information on these matters here. Note that the study will require separate approval by the Research Governance Office.

Technical details
If one or more Study Characteristics in categories M.3 to M.7 or H applies, provide the description of the technical details of the experimental or study design, the power calculation(s) which yield the required sample size(s), and how the data will be analysed, as separate appendices.

CHECKLIST OF DOCUMENTS TO UPLOAD

Please provide the following forms, naming the files as explicitly as possible, e.g., "Participant Information", "Questionnaire", "Consent Form", "DPA Plan", "Permission to contact", "Risk Management Plan", "Debrief Plan", "Contact Information", and/or "Technical details" as appropriate. Each document must specify the reference number in the form ERGO/FEPS/xxxx, the document version number, and its date of last edit.

i) **Participant Information** in the form that it will be given to **participants**.
ii) Data collection method (e.g. for secondary data or "big data") **/ Participant** Questionnaire in the form that it will be given to **participants**.
iii) **Consent Form** (or consent information if no **personal data** is collected) in the form that it will be given to **participants**.
iv) **DPA Plan**.
v) Evidence of permission to contact (prospective) **participants** through any third party.
vi) **Risk Management Plan**.
vii) **Debrief Plan**.
viii) **Contact Information**.
ix) Technical details of the experimental or study design, the power calculation(s) for the required sample size(s), and how the data will be analysed.
x) Further details and justifications in the case of: **invasive** equipment, material(s), or process(es); **participants** who are not able to withdraw at any time and for any reason; animals; human tissue; or biological samples.

Appendix Q

CIST Game ERGO 64746 Ethics Application

Status: Approved

The end date for this study was 30th July 2021. This ethical approval covers the event held on the University Campus on the 9th of July 2021, following Covid-19 guidelines, see Section 8.6 CIST study realisation.

UNIVERSITY OF Southampton

FEPS Ethics Committee
FEPS EC Application Form Ver 2

Reference number: **ERGO**/FEPS/**64746**	Submission version: 1	Date: 06-05-2021
Name of investigator(s): **Mr Stephen Hart**		
Name of supervisor(s) (if student investigator(s)): **Dr Basel Halak**		
Title of study: **CIST A Serious Game for Hardware Security Supply Chain**		

Note that failure to follow the University's policy on Ethics may lead to disciplinary action concerning Misconduct or a breach of Academic Integrity.
By submitting this application, the investigator(s) undertake to:

- Conduct the study in accordance with University policies governing:
  Ethics (http://www.southampton.ac.uk/ris/policies/ethics.html);
  Data management (http://www.southampton.ac.uk/library/research/researchdata/);
  Health and Safety (http://www.southampton.ac.uk/healthandsafety);
  Academic Integrity (http://www.calendar.soton.ac.uk/sectionIV/academic-integrity-statement.html.
- Ensure the study Reference number ERGO/FEPS/44919 is prominently displayed on all advertising and study materials, and is reported on all media and in all publications;
- Conduct the study in accordance with the information provided in the application, its appendices, and any other documents submitted;
- Submit the study for re-review (as an amendment through ERGO) or seek FPSE EC advice if any changes, circumstances, or outcomes materially affect the study or the information given;
- Promptly advise an appropriate authority (Research Governance Office) of any adverse study outcomes (via an adverse event notification through ERGO);
- Submit an end-of-study form if required to do so.

REFER TO THE INSTRUCTIONS AND GUIDE DOCUMENTS WHEN COMPLETING THIS FORM AND THE TEMPLATES DOCUMENT WHEN PREPARING THE REQUIRED APPENDICES.

STUDY DETAILS

What are the aims and objectives of this study?
To test the educational effectiveness of a serious cyber game called CIST, which was created using a design model called MOTENS that is used to design serious cyber games. The results of the study to be published in a scientific journal or conference paper.

Background of the study (a brief rationale for conducting the study)
This questionnaire is to collect impressions about the CIST serious game and test the educational effectiveness of the game and, therefore, the pedagogical model MOTENS used to design and create the game. This is very targeted within the cyber research community University, Government & private companies) that would use models to design serious cyber games. MOTENS model was created by the applicant of this ERGO submission and evaluated in a previous ERGO submission (Reference Number: ERGO/FPSE/62140) as part of previous research with the University Southampton.

Key research question (Specify hypothesis if applicable)
To test the educational effectiveness of the serious game CIST, which is a single-player Game to teach threats, vulnerabilities, and countermeasures to the IC Supply Chain. This will assist in the evaluation of the MOTENS pedagogical model to design serious cyber games for education.

Study design (Give a brief outline of the study design and why it is being used)
The design questionnaire is in two parts: The first part is about the background of respondents (anonymised) and asks their team/function area they work, interest in serious games, expertise in threats in IC supply chain and expertise in hardware security education and awareness. The second part of the questionnaire study design uses the technology assessment model (TAM) to ask questions to test the CIST game, perceived usefulness, perceived ease of use and intention to use.

Pre-STUDY

Characterise the proposed participants
The participants will be known to the researcher or supervisors. They will be working in the area of cyber security research either: University as Professor; Associate Professor or Lecturer; University in the Research Department, for UK Government in the Research Department, Organisation in the Research Department, PhD student or BSc/MSC students within Southampton University.

Describe how participants will be approached

If any e-mail lists are used, including FEPS distribution lists, justify their use here
They will be sent an email inviting them to take part no distribution lists will be used, or any emails collected from previous research. The participants are known to the research student or supervisors. The emails will be sent using blind copy (Bcc), direct to the participant to ensure no email addresses are revealed to other recipients or internal Southampton University email groups.

A one-day event will be run in June 2021 by Southampton University ECS department for BSc & MSc students, and as part of this event, they will be given the CIST game to play with players who successfully win the game entered into a prize draw for a nominal prize and all player invited to complete a questionnaire and give anonymous feedback. The completion of the questionnaire and feedback is not mandatory.

We will also have some presentations of the CIST game to Southampton University research groups/teams with a request to complete an anonymous questionnaire.

Describe how inclusion and/or exclusion criteria will be applied (if any)

Participants may feel this is not their research area of interest and can exclude themselves as participation is voluntary. Students at the ECS day event can play the CIST game but not required to complete the feedback form.

No exclusion criteria will be applied, but the inclusion is as follows:

- Participants will be known to student researcher or supervisors
- Participants may forward a request to another person in the organisation working within the cyber research area
- Participants will all be working in the area of cyber security research or education and awareness

Describe how participants will decide whether to take part

If the participants decide to take part, they will be requested to email the questionnaire back to the research student using the Southampton University email address. Some participants may decide to email the supervisor via University email address, who will forward the email to the research student. It is also possible that some participants may return more than one completed questionnaire. This is acceptable as the questionnaires are anonymous and only need to verify the questionnaire came from a validated source. Some participants and some students etc., prefer using anonymous online forms, and if required, the same form can be provided using Southampton University Office 365. If this option is used, the option to record name will be turned off and form will be anonymous. For the ECS day event the participants and simply hand back the anonymous questionnaire.

Participant Information (Appendix (i))

Provide the Participant Information in the form that it will be given to participants as Appendix (i). All studies must provide participant information.

Consent Form/Information (Appendix (iii))

Provide the Consent Form (or the request for consent) in the form that it will be given to participants as Appendix (iii). All studies must obtain participant consent. Some studies may obtain verbal consent (and only present consent information), other studies will require written consent, as explained in the Instructions, Guide, and Templates documents.

DURING THE STUDY

Describe the study procedures as they will be experienced by the participant
The participant, if external to the University of Southampton, will receive an email with a request to participate. The email will contain a link to the CIST game https://mygame.page/cist-game. The participant can then decide to complete the attached questionnaire (word version). They can return if they decide to take part or ignore the email, and they will not be contacted. For the ECS event, day players will be given time to play the CIST game and the opportunity to provide anonymous feedback in comments and questionnaire. There is also a brief PowerPoint presentation explaining the CIST game and common hardware threats.

Identify how, when, where, and what kind of data will be recorded (not just the formal research data, but including all other study data such as e-mail addresses and signed consent forms)
No personal data, such as emails address etc., will be collected. The background questions cannot identify the participant and questions on the CIST game using the Likert scale. There is an area on the form titled “Please enter any additional comments further information. “, if participants give identifiable information, this will not be used in the research. If the form needs to be shared internally within Southampton University, then if participant used identifiable information, this will be redacted.

Participant questionnaire/data gathering methods (Appendix (ii))

As Appendix (ii), reproduce any and all participant questionnaires or data gathering instruments in the exact forms that they will be given to or experienced by participants. If conducting less formal data collection, or data collection that does not involve direct questioning or observation of participants (e.g. secondary data or “big data”), provide specific information concerning the methods that will be used to obtain the data of the study.

POST STUDY

Identify how, when, and where data will be stored, processed, and destroyed
Does not apply.

STUDY CHARACTERISTICS

(L.1) The study is funded by a commercial organisation: **No** (delete one) If 'Yes', provide details of the funder or funding agency here.

(L.2) There are restrictions upon the study: **No** (delete one) If 'Yes', explain the nature and necessity of the restrictions here.

(L.3) Access to participants is through a third party: **No** (delete one)
If 'Yes', provide evidence of your permission to contact them as Appendix (v). Do not provide explanation or information on this matter here.

(M.1) Personal data is or *may be collected or processed: **No** (delete one) Data will be processed outside the UK: No (delete one) If 'Yes' to either question, provide the DPA Plan as Appendix (iv). Do not provide information or explanation on this matter here. Note that using or recording e-mail addresses, telephone numbers, signed consent forms, or similar study-related personal data requires M.1 to be "Yes". (* Secondary data / "big data" may be de-anonymised, or may contain personal data. If so, answer 'Yes'.)

(M.2) There is inducement to participants: **No** (delete one) If 'Yes', explain the nature and necessity of the inducement here.

(M.3) The study is intrusive: **No** (delete one) If 'Yes', provide the Risk Management Plan, the Debrief Plan, and Technical Details as Appendices (vi), (vii), and (ix), and explain here the nature and necessity of the intrusion(s).

(M.4) There is risk of harm during the study: **No** (delete one) If 'Yes', provide the Risk Management Plan, the Contact Information, the Debrief Plan, and Technical Details as Appendices (vi), (vii), (viii), and (ix), and explain here the necessity of the risks.

(M.5) The true purpose of the study will be hidden from participants: **No** (delete one) The study involves deception of participants: **No** (delete one) If 'Yes' to either question, provide the Debrief Plan and Technical Details as Appendices (vii) and (ix), and explain here the necessity of the deception.

(M.6) Participants may be minors or otherwise have diminished capacity: **No** (delete one) If 'Yes', AND if one or more Study Characteristics in categories M or H applies, provide the Risk Management Plan, the Contact Information, and Technical Details as Appendices (vi), (vii), & (ix), and explain here the special arrangements that will ensure informed consent.

(M.7) Sensitive data is collected or processed: **No** (delete one) If 'Yes', provide the DPA Plan and Technical Details as Appendices (iv) and (ix). Do not provide explanation or information on this matter here.

(H.1) The study involves: invasive equipment, material(s), or process(es); or participants who are not able to withdraw at any time and for any reason; or animals; or human tissue; or biological samples: **No** (delete one) If 'Yes', provide Technical Details and further justifications as Appendices (ix) and (x). Do not provide explanation or information on these matters here. Note that the study will require separate approval by the Research Governance Office.

Technical details
If one or more Study Characteristics in categories M.3 to M.7 or H applies, provide the description of the technical details of the experimental or study design, the power calculation(s) which yield the required sample size(s), and how the data will be analysed, as separate appendices.

CHECKLIST OF DOCUMENTS TO UPLOAD

Please provide the following forms, naming the files as explicitly as possible, e.g., "Participant Information", "Questionnaire", "Consent Form", "DPA Plan", "Permission to contact", "Risk Management Plan", "Debrief Plan", "Contact Information", and/or "Technical details" as appropriate. Each document must specify the reference number in the form ERGO/FEPS/xxxx, the document version number, and its date of last edit.

i) **Participant** Information in the form that it will be given to **participants**.
ii) Data collection method (e.g. for secondary data or "big data") **/ Participant** Questionnaire in the form that it will be given to **participants**.
iii) **Consent Form** (or consent information if no **personal data** is collected) in the form that it will be given to **participants**.
iv) **DPA Plan**.
v) Evidence of permission to contact (prospective) participants through any third party.
vi) **Risk Management Plan**.
vii) **Debrief Plan**.
viii) **Contact Information**.
xi) Technical details of the experimental or study design, the power calculation(s) for the required sample size(s), and how the data will be analysed.
x) Further details and justifications in the case of: **invasive** equipment, material(s), or process(es); **participants** who are not able to withdraw at any time and for any reason; animals; human tissue; or biological samples.

Bibliography

Aladawy, D., Beckers, K., and Pape, S. (2018). PERSUADED: fighting social engineering attacks with a serious game. In *15th International Conference in Trust, Privacy and Security in Digital Business*, volume 11033 of *LNCS*, pages 103–118. Springer. https://doi.org/10.1007/978-3-319-98385-1_8.

Amory, A. (2007). Game object model version ii: a theoretical framework for educational game development. *Educational Technology Research and Development*, 55(1):51–77. https://doi.org/10.1007/s11423-006-9001-x.

Arnab, S., Lim, T., Carvalho, M. B., Bellotti, F., De Freitas, S., Louchart, S., Suttie, N., Berta, R., and De Gloria, A. (2015). Mapping learning and game mechanics for serious games analysis. *British Journal of Educational Technology*, 46(2):391–411. https://doi.org/10.1111/bjet.12113.

Atorf, D., Kannegieser, E., and Roller, W. (2019). Study on enhancing learnability of a serious game by implementing a pedagogical agent. In *International Conference on Games and Learning Alliance*, pages 158–168. Springer. https://doi.org/10.1007/978-3-030-34350-7_16.

Bada, S. O. and Olusegun, S. (2015). Constructivism learning theory: A paradigm for teaching and learning. *Journal of Research & Method in Education*, 5(6):66–70. https://api.semanticscholar.org/CorpusID:37780480.

Bakhuys Roozeboom, M., Visschedijk, G., and Oprins, E. (2017). The effectiveness of three serious games measuring generic learning features. *British journal of educational technology*, 48(1):83–100. https://doi.org/10.1111/bjet.12342.

Beckers, K. and Pape, S. (2016). A serious game for eliciting social engineering security requirements. In *Requirements Engineering Conference (RE), 2016 IEEE 24th International*, pages 16–25. IEEE. https://doi.org/10.1109/RE.2016.39.

Bíró, G. I. (2014). Didactics 2.0: A pedagogical analysis of gamification theory from a comparative perspective with a special view to the components of learning. *Procedia-Social and Behavioral Sciences*, 141:148–151. https://doi.org/10.1016/j.sbspro.2014.05.027.

Bloom, B. S. et al. (1956). Taxonomy of educational objectives. vol. 1: Cognitive domain. *New York: McKay*, 20:24.

Carvalho, M. B., Bellotti, F., Berta, R., De Gloria, A., Sedano, C. I., Hauge, J. B., Hu, J., and Rauterberg, M. (2015). An activity theory-based model for serious games analysis and conceptual design. *Computers & education*, 87:166–181. http://dx.doi.org/10.1016/j.compedu.2015.03.023.

Chalmers, A. and Debattista, K. (2009). Level of realism for serious games. In *2009 Conference in Games and Virtual Worlds for Serious Applications*, pages 225–232. IEEE. https://doi.org/10.1109/VS-GAMES.2009.43.

Charsky, D. (2010). From edutainment to serious games: A change in the use of game characteristics. *Games and culture*, 5(2):177–198. https://doi.org/10.1177%2F1555412009354727.

CIAS (2021). Cyber Threat Defender. http://cias.utsa.edu/ctd.php.

CIS (2021). Center Internet Security: Top 18 Critical Security Controls for Effective Cyber Defense. https://www.cisecurity.org/controls/cis-controls-list/.

Conejo, G. G., Gasparini, I., and da Silva Hounsell, M. (2019). Detailing motivation in a gamification process. In *2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT)*, volume 2161, pages 89–91. IEEE. https://doi.org/10.1109/ICALT.2019.00031.

Continuity, B. and Forum, R. (3rd February 2018). Government sets the bar for cyber risk with cyber essentials. http://www.continuityforum.org/content/news/178023/government-sets-bar-cyber-risk-cyber-essentials.

Creative Commons (2018). License for use of Elevation of Privilege (EoP) Card Game. https://creativecommons.org/licenses/by/3.0/us/.

Cryptomancer RPG (3rd February 2018). a tabletop role-playing game made for hackers, by hackers. http://cryptorpg.com.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, pages 319–340. https://doi.org/10.2307/249008.

Deci, E. L. and Ryan, R. M. (2008). Self-determination theory: A macrotheory of human motivation, development, and health. *Canadian psychology/Psychologie canadienne*, 49(3):182. https://doi.org/10.1037/a0012801.

Denning, T., Lerner, A., Shostack, A., and Kohno, T. (2013). Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 915–928. ACM. https://doi.org/10.1145/2508859.2516753.

Deterding, S. (2012). Gamification: designing for motivation. *Interactions*, 19(4):14–17. https://doi.org/10.1145/2212877.2212883.

Deterding, S., Dixon, D., Khaled, R., and Nacke, L. (2011a). From game design elements to gamefulness: defining "gamification". In *Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments*, pages 9–15. https://doi.org/10.1145/2181037.2181040.

Deterding, S., Sicart, M., Nacke, L., O'Hara, K., and Dixon, D. (2011b). Gamification. using game-design elements in non-gaming contexts. *Association for Computing Machinery*, pages 2425–2428. http://dx.doi.org/10.1145/1979742.1979575.

Di, J. and Smith, S. (2007). A hardware threat modeling concept for trustable integrated circuits. In *2007 IEEE Region 5 Technical Conference*, pages 354–357. IEEE. https://doi.org/10.1109/TPSD.2007.4380353.

Dindar, M., Ren, L., and Järvenoja, H. (2021). An experimental study on the effects of gamified cooperation and competition on english vocabulary learning. *British Journal of Educational Technology*, 52(1):142–159. https://doi.org/10.1111/bjet.12977.

Driscoll, M. P. (2000). Psychology of learning for instruction. *Boston, Allyn and Bacon*, pages 373–396. ISBN 0205263216.

Duffy, T. M. and Jonassen, D. H. (2013). *Constructivism and the technology of instruction: A conversation*. Routledge. ISBN 9780805812725.

Engeström, Y. (2015). *Learning by expanding*. Cambridge University Press. https://doi.org/10.1017/CBO9781139814744.

European Union (EU) (3rd February 2018). General Data Protection Regulation (EU) 2016/679. https://gdpr-info.eu/.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., and Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86:13–23. https://doi.org/10.1016/j.dss.2016.02.012.

Fosnot, C. T. and Perry, R. S. (1996). Constuctivism: A psychological theory of learning. In *Constructivism: Theory, Perspectives. and Practice*, chapter 2, pages 9–38. Teachers College Pres. ISBN 0807745707.

Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., and 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*. https://doi.org/10.1109/TSE.2017.2782813.

Gagné, M. and Deci, E. L. (2005). Self-determination theory and work motivation. *Journal of Organizational behavior*, 26(4):331–362. https://doi.org/10.1002/job.322.

Gagné, R. M. and Briggs, Leslie J, W. W. (1992). *Principles of instructional design*. Harcourt Brace College Publishers. ISBN 0030347572.

Gondree, M., Peterson, Z. N., and Denning, T. (2013). Security through play. *IEEE Security & Privacy*, 11(3):64–67. https://doi.org/10.1109/MSP.2013.69.

González-Tablas, A. I., González Vasco, M. I., Cascos, I., and Planet Palomino, Á. (2020). Shuffle, cut, and learn: Crypto go, a card game for teaching cryptography. *Mathematics*, 8(11):1993. https://doi.org/10.3390/math8111993.

Goodenough, A. and Waite, S. (2012). Real world research: a resource for users of social research methods in applied settings. *Taylor & Francis*. https://doi.org/10.1080/02607476.2012.708121.

Graffer, I., Bartnes, M., and Bernsmed, K. (2015). Play2prepare: A board game supporting it security preparedness exercises for industrial control organizations. https://ojs.bibsys.no/index.php/NISK/article/view/297.

Hainey, T., Connolly, T. M., Boyle, E. A., Wilson, A., and Razak, A. (2016). A systematic literature review of games-based learning empirical evidence in primary education. *Computers & Education*, 102:202–223. https://doi.org/10.1016/j.compedu.2016.09.001.

Halak, B. (2021). *Hardware Supply Chain Security: Threat Modelling, Emerging Attacks and Countermeasures*. Springer Nature. https://www.springer.com/gp/book/9783030627065.

Hart, S., Margheri, A., Paci, F., and Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95:101827. http://dx.doi.org/10.1016/j.cose.2020.101827.

Hendrix, M., Al-Sherbaz, A., and Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games*, 3(1). http://dx.doi.org/10.17083/ijsg.v3i1.107.

Hill, W., Fanuel, M., and Yuan, X. (2020). Comparing serious games for cyber security education. *2020 ASEE Southeastern Section Conference*. https://sites.asee.org/se/wp-content/uploads/sites/56/2021/01/2020ASEESE117.pdf.

Holdsworth, J. and Apeh, E. (2017). An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. In *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*, pages 111–117. IEEE. https://doi.org/10.1109/REW.2017.47.

Hursen, C. and Bas, C. (2019). Use of gamification applications in science education. *International Journal of emerging technologies in Learning*, 14(1). https://doi.org/10.3991/ijet.v14i01.8894.

IEC (2021). International Electrotechnical Commission 62443 Security for industrial automation and control systems. https://webstore.iec.ch/publication/33615.

Ip, B. and Jacobs, G. (2005). Segmentation of the games market using multivariate analysis. *Journal of Targeting, Measurement and Analysis for Marketing*, 13(3):275–287. https://doi.org/10.1057/palgrave.jt.5740154.

Irvine, C. E., Thompson, M. F., and Allen, K. (2005). Cyberciege: Gaming for information assurance. *IEEE Security & Privacy*, 3(3):61–64. https://doi.org/10.1109/MSP.2005.64.

ISO/IEC (2018). ISO/IEC 27005:2018 Information technology – Security techniques - Information security risk management. https://www.iso.org/standard/75281.html.

ISO/IEC (2021). ISO/IEC 27001 Information Security Management. https://www.iso.org/isoiec-27001-information-security.html.

Jaffray, A., Finn, C., and Nurse, J. R. (2021). Sherlocked: A detective-themed serious game for cyber security education. *Springer*. https://doi.org/10.1007/978-3-030-81111-2_4.

Jang, Y., Lee, J., Lee, S., and Kim, T. (2017). Sgx-bomb: Locking down the processor via rowhammer attack. In *Proceedings of the 2nd Workshop on System Software for Trusted Execution*, pages 1–6. https://doi.org/10.1145/3152701.3152709.

Jonassen, D. H. and Rohrer-Murphy, L. (1999). Activity theory as a framework for designing constructivist learning environments. *Educational technology research and development*, 47(1):61–79. https://doi.org/10.1007/BF02299477.

Joshi, A., Kale, S., Chandel, S., and Pal, D. K. (2015). Likert scale: Explored and explained. *Current Journal of Applied Science and Technology*, pages 396–403. https://doi.org/10.9734/BJAST/2015/14975.

Khan, B., Alghathbar, K. S., Nabi, S. I., and Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5(26):10862–10868. https://doi.org/10.5897/AJBM11.067.

Khatibi, M. B., Badeleh, A., and Khodabandelou, R. (2021). A bibliometric analysis on the research trends of gamification in higher education: 2010–2020. *The New Educational Review*, 65(3):17–28.

Kocher, P., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M., and Yarom, Y. (2018). Spectre attacks: Exploiting speculative execution. https://arxiv.org/abs/1801.01203v1.

Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, 24(1-3):72–77. https://doi.org/10.1080/19393555.2015.1051676.

Labunets, K., Massacci, F., Paci, F., and 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*, pages 163–172. https://doi.org/10.1109/ESEM.2013.29.

Labunets, K., Paci, F., Massacci, F., and 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*, pages 28–35. https://doi.org/10.1109/EmpiRE.2014.6890113.

Le Compte, A., Elizondo, D., and Watson, T. (2015). A renewed approach to serious games for cyber security. In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, pages 203–216. IEEE. https://doi.org/10.1109/CYCON.2015.7158478.

Lim, T., Carvalho, M. B., Bellotti, F., Arnab, S., De Freitas, S., Louchart, S., Suttie, N., Berta, R., and De Gloria, A. (2015). The LM-GM framework for serious games analysis. *Pittsburgh: University of Pittsburgh*. https://api.semanticscholar.org/CorpusID:18789355.

Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., and Hamburg, M. (2018). Meltdown. https://arxiv.org/abs/1801.01207v1.

Liu, T.-Y. and Chu, Y.-L. (2010). Using ubiquitous games in an english listening and speaking course: Impact on learning outcomes and motivation. *Computers & Education*, 55(2):630–643. https://doi.org/10.1016/j.compedu.2010.02.023.

Lorås, M. (2017). Let the gamification begin! - A qualitative case study of student experiences in the gamified learning environment Heimdall's Quest. Master's thesis, NTNU. http://hdl.handle.net/11250/2450803.

Luo, Z. (2021). Educational gamification from 1995 to 2020: A bibliometric analysis. *2021 the 6th International Conference on Distance Education and Learning*, pages 140–145. https://doi.org/10.1145/3474995.3475740.

Malli Mohan, K. (2010). *Outsourcing trends in semiconductor industry*. PhD thesis, Massachusetts Institute of Technology. http://hdl.handle.net/1721.1/62770.

Mancuso, V. F., Hamilton, K., Tesler, R., Mohammed, S., and McNeese, M. (2013). An experimental evaluation of the effectiveness of endogenous and exogenous fantasy in computer-based simulation training. *International Journal of Gaming and Computer-Mediated Simulations (IJGCMS)*, 5(1):50–65. http://dx.doi.org/10.4018/jgcms.2013010104.

Maor, D. (1999a). A teacher professional development program on using a constructivist multimedia learning environment. *Learning Environments Research*, 2(3):307–330. https://doi.org/10.1023/A:1009915305353.

Maor, D. (1999b). Teachers-as-learners: The role of a multimedia professional development program in changing classroom practice. *Australian Science Teachers' Journal*, 45. http://researchrepository.murdoch.edu.au/id/eprint/8718.

Martí-Parreño, J., Méndez-Ibáñez, E., and Alonso-Arroyo, A. (2016). The use of gamification in education: a bibliometric and text mining analysis. *Journal of computer assisted learning*, 32(6):663–676. https://doi.org/10.1111/jcal.12161.

Mayer, I., Bekebrede, G., Harteveld, C., Warmelink, H., Zhou, Q., Van Ruijven, T., Lo, J., Kortmann, R., and Wenzler, I. (2014). The research and evaluation of serious games: Toward a comprehensive methodology. *British journal of educational technology*, 45(3):502–527. https://doi.org/10.1111/bjet.12067.

McGonigal, J. (2011). *Reality is broken: Why games make us better and how they can change the world*. Penguin. ISBN 0099540282.

McKinsey (2019). McKinsey on semiconductors creating value, pursuing innovation, and optimizing operations. https://www.mckinsey.com/~/media/McKinsey/Industries/Semiconductors/Our%20Insights/McKinsey%20on%20Semiconductors%20Issue%207/McK_Semiconductors_Oct2019-Full%20Book-V12-RGB.ashx.

Mestadi, W., Nafil, K., Touahni, R., and Messoussi, R. (2018). An assessment of serious games technology: toward an architecture for serious games design. *International Journal of Computer Games Technology*, 2018. https://doi.org/10.1155/2018/9834565.

Microsoft (2018). Elevation of privilege (eop) card game. https://www.microsoft.com/en-us/SDL/adopt/eop.aspx.

Mitgutsch, K. and Alvarado, N. (2012). Purposeful by design?: a serious game design assessment framework. In *Proceedings of the International Conference on the foundations of digital games*, pages 121–128. ACM. https://doi.org/10.1145/2282338.2282364.

Mitnick, K. D. and Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Moore, A. P., Ellison, R. J., and Linger, R. C. (2001). Attack modeling for information security and survivability. Technical report, Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst. https://apps.dtic.mil/sti/citations/ADA388771.

Mora, A., Riera, D., Gonzalez, C., and Arnedo-Moreno, J. (2015). A literature review of gamification design frameworks. In *2015 7th International Conference on Games and Virtual Worlds for Serious Applications (VS-Games)*, pages 1–8. IEEE. https://doi.org/10.1109/VS-GAMES.2015.7295760.

Moreno-Ger, P., Burgos, D., Martínez-Ortiz, I., Sierra, J. L., and Fernández-Manjón, B. (2008). Educational game design for online education. *Computers in Human Behavior*, 24(6):2530–2540. https://doi.org/10.1016/j.chb.2008.03.012.

Morschheuser, B., Hamari, J., and Maedche, A. (2019). Cooperation or competition–when do people contribute more? a field experiment on gamification of crowdsourcing. *International*

Journal of Human-Computer Studies, 127:7–24. https://doi.org/10.1016/j.ijhcs.2018.10.001.

Nacke, L. E. and Deterding, S. (2017). The maturing of gamification research. *Computers in Human Behavior*, 71:450–454. https://doi.org/10.1016/j.chb.2016.11.062.

Nagarajan, A., Allbeck, J. M., Sood, A., and Janssen, T. L. (2012). Exploring game design for cybersecurity training. In *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, pages 256–262. IEEE. https://doi.org/10.1109/CYBER.2012.6392562.

NCSC (2021). National Cyber Security Centre: 10 Step to Cyber Security: Guidance on how organisations can protect themselves in cyberspace. https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security.

NCSE (2020). National Cyber Security Centre: Cyber Essentials scheme and certification. https://www.ncsc.gov.uk/cyberessentials/overview.

Neck, H. M. and Greene, P. G. (2011). Entrepreneurship education: known worlds and new frontiers. *Journal of small business management*, 49(1):55–70.

Neghina, D.-E. and Scarlat, E. (2013). Managing information technology security in the context of cyber crime trends. *International journal of computers communications & control*, 8(1):97–104. https://doi.org/10.15837/ijccc.2013.1.173.

Nguyen, T. A. and Pham, H. (2020). A design theory-based gamification approach for information security training. In *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, pages 1–4. IEEE. https://doi.org/10.1109/RIVF48685.2020.9140730.

NIST (2011). National Institute of Standards and Technologies: Managing Information Security Risk Organization, Mission, and Information System View. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf.

NIST (2021a). National Institute of Standards and Technologies: Cyber Security Framework. https://www.nist.gov/cyberframework.

NIST (2021b). National Institute of Standards and Technologies: Cyber Security Framework - Five Functions. https://www.nist.gov/cyberframework/online-learning/five-functions.

OASIS (25th September 2019). Structured Threat Information eXpression (STIX™). https://stixproject.github.io/.

OECD (2019). Organisation for Economic Co-operation and Development: Trade in Counterfeit Products and the UK Economy. http://www.oecd.org/governance/risk/trade-in-counterfeit-products-and-the-uk-economy-2019.htm.

OWASP (2021). Open Web Application Security Project, Cornucopia. https://www.owasp.org/index.php/OWASP_Cornucopia.

Paharia, R. (2012). Gamification means amplifying intrinsic value. *Interactions*, 19(4):17.

Perkins, D. N. (1991). What constructivism demands of the learner. *Educational technology*, 31(9):19–21. https://www.jstor.org/stable/44401693.

Qasrawi, R. and BeniAbdelrahman, A. (2020). The higher and lower-order thinking skills (hots and lots) in unlock english textbooks (1st and 2nd editions) based on bloom's taxonomy: An analysis study. *International Online Journal of Education and Teaching*, 7(3):744–758. https://iojet.org/index.php/IOJET/article/view/866.

Rapeepisarn, K., Wong, K. W., Fung, C. C., and Khine, M. S. (2008). The relationship between game genres, learning techniques and learning styles in educational computer games. In *International conference on technologies for E-learning and digital entertainment*, pages 497–508. Springer. https://doi.org/10.1007/978-3-540-69736-7_53.

Rieb, A. and Lechner, U. (2016). Operation digital chameleon: Towards an open cybersecurity method. In *Proceedings of the 12th International Symposium on Open Collaboration*, page 7. ACM. https://doi.org/10.1145/2957792.2957800.

Robson, C. and McCartan, K. (2016). *Real world research: a resource for users of social research methods in applied settings*. Wiley. ISBN 987-1-4051-82409.

Roepke, R. and Schroeder, U. (2019). The problem with teaching defence against the dark arts: A review of game-based learning applications and serious games for cyber security education. In *CSEDU (2)*, pages 58–66. http://dx.doi.org/10.5220/0007706100580066.

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

Rooney, P. (2012). A theoretical framework for serious game design: exploring pedagogy, play and fidelity and their implications for the design process. *International Journal of Game-Based Learning (IJGBL)*, 2(4):41–60. https://doi.org/10.4018/ijgbl.2012100103.

Routledge, H. (2016). *Why games are good for business: How to leverage the power of serious games, gamification and simulations*. Springer. ISBN 1137448962.

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., and Wu, Q. (2010). A survey of game theory as applied to network security. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pages 1–10. IEEE. https://doi.org/10.1109/HICSS.2010.35.

Savvani, S. and Liapis, A. (2019). A participatory approach to redesigning games for educational purposes. In *International Conference on Games and Learning Alliance*, pages 13–23. Springer. https://doi.org/10.1007/978-3-030-34350-7_2.

Seng, T. (2000). Reflecting on innovating the academic architecture for the 21st century. *Educational Developments*, 1:8–10.

Seng Tan*, O. (2004). Students' experiences in problem-based learning: three blind mice episode or educational innovation? *Innovations in Education and Teaching International*, 41(2):169–184. https://doi.org/10.1080/1470329042000208693.

Shostack, A. (2008). Experiences threat modeling at microsoft. *MODSEC@MoDELS*, 2008. https://api.semanticscholar.org/CorpusID:2508643.

Shostack, A. (2014). Elevation of Privilege: Drawing Developers into Threat Modeling. In *Summit on Gaming, Games, and Gamification in Security Education*. USENIX Association. https://api.semanticscholar.org/CorpusID:17227023.

Shreeve, B., Hallett, J., Edwards, M., Ramokapane, K. M., Atkins, R., and Rashid, A. (2020). The best laid plans or lack thereof: Security decision-making of different stakeholder groups. *IEEE Transactions on Software Engineering*, pages 1–1. https://doi.org/10.1109/TSE.2020.3023735.

Singh, A. A. and Singh, K. S. (2012). Network threat ratings in conventional dread model using fuzzy logic. *International Journal of Computer Science Issues (IJCSI)*, 9(1):478. https://api.semanticscholar.org/CorpusID:147768738.

Spiro, R. J., Collins, B. P., Thota, J. J., and Feltovich, P. J. (2003). Cognitive flexibility theory: Hypermedia for complex learning, adaptive knowledge application, and experience acceleration. *Educational technology*, 43(5):5–10. https://www.jstor.org/stable/44429454.

Stott, A. and Neustaedter, C. (2013). Analysis of gamification in education. *Surrey, BC, Canada*, 8:36. https://api.semanticscholar.org/CorpusID:30967088.

Symantec (2019). Internet Security Threat Report, Volume 24 February 2019 (ISTR). https://www.broadcom.com/support/security-center/publications/archive.

Tamara Denning, Batya Friedman, and Tadayoshi Kohno (2021). The Security Cards. http://securitycards.cs.washington.edu/.

ThinkFun (2021). Hacker, Cybersecurity logic game. https://www.thinkfun.com/learn-coding/hacker/.

Thomas, M. K., Shyjka, A., Kumm, S., and Gjomemo, R. (2019). Educational design research for the development of a collectible card game for cybersecurity learning. *Journal of Formative Design in Learning*, pages 1–12. https://doi.org/10.1007/s41686-019-00027-0.

Thompson, M. and Irvine, C. (2011). Active learning with the cyberciege video game. In *Proceedings of the 4th Conference on Cyber Security Experimentation and Test*, pages 10–10. USENIX Association. http://hdl.handle.net/10945/40296.

Thompson, M. and Takabi, H. (2016). Effectiveness of using card games to teach threat modeling for secure web application developments. *Issues in Information Systems*, 17(3). https://doi.org/10.48009/3_iis_2016_244-253.

Trinidad, M., Ruiz, M., and Calderón, A. (2021). A bibliometric analysis of gamification research. *IEEE Access*, 9:46505–46544. https://doi.org/10.1109/ACCESS.2021.3063986.

Tupsamudre, H., Wasnik, R., Biswas, S., Pandit, S., Vaddepalli, S., Shinde, A., Gokul, C., Banahatti, V., and Lodha, S. (2018). GAP: A game for improving awareness about passwords. In *Joint International Conference on Serious Games*, pages 66–78. Springer. https://doi.org/10.1007/978-3-030-02762-9_8.

Tuunanen, J. and Hamari, J. (2012). Meta-synthesis of player typologies. In *Proceedings of Nordic Digra 2012 Conference: Games in Culture and Society, Tampere, Finland*. http://www.digra.org/digital-library/publications/meta-synthesis-of-player-typologies/.

Vermeulen, H., Gain, J., Marais, P., and ODonovan, S. (2016). Reimagining gamification through the lens of activity theory. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 1328–1337. IEEE. https://doi.org/10.1109/HICSS.2016.168.

Williams, I. and Yuan, X. (2015). Evaluating the effectiveness of microsoft threat modeling tool. In *Proceedings of the 2015 Information Security Curriculum Development Conference*, page 9. ACM. https://doi.org/10.1145/2885990.2885999.

Williams, L., Meneely, A., and Shipley, G. (2010). Protection poker: The new software security" game". *IEEE Security & Privacy*, 8(3):14–20. https://doi.org/10.1109/MSP.2010.58.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wesslén, A. (2012). *Experimentation in software engineering*. Springer Science & Business Media. ISBN 3642432263.

Wuyts, K., Scandariato, R., and Joosen, W. (2014). Empirical evaluation of a privacy-focused threat modeling methodology. *Journal of Systems and Software*, 96:122–138. https://doi.org/10.1016/j.jss.2014.05.075.

Wuyts, K., Sion, L., and Joosen, W. (2020). Linddun go: A lightweight approach to privacy threat modeling. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 302–309. IEEE. https://doi.org/10.1109/EuroSPW51379.2020.00047.

Xiao, Y., Zhang, X., Zhang, Y., and Teodorescu, R. (2016). One bit flips, one cloud flops: Cross-vm row hammer attacks and privilege escalation. In *25th {USENIX} security symposium ({USENIX} security 16)*, pages 19–35. https://api.semanticscholar.org/CorpusID:9001439.

Yasin, A., Liu, L., Li, T., Fatima, R., and Wang, J. (2019). Improving software security awareness using a serious game. *IET Software*, 13(2):159–169. https://doi.org/10.1049/iet-sen.2018.5095.

Yusoff, A. (2010). *A conceptual framework for serious games and its validation*. PhD thesis, University of Southampton. http://eprints.soton.ac.uk/id/eprint/171663.

Yusoff, A., Crowder, R., and Gilbert, L. (2010). Validation of serious games attributes using the technology acceptance model. In *2010 Second International Conference on Games and Virtual Worlds for Serious Applications*, pages 45–51. IEEE. https://doi.org/10.1109/VS-GAMES.2010.7.

Z-Man Games (2021). Pandemic game. https://zmangames.com/en/games/pandemic/.

Zhang, X., Wuwong, N., Li, H., and Zhang, X. (2010). Information security risk management framework for the cloud computing environments. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, pages 1328–1334. IEEE. https://doi.org/10.1109/CIT.2010.501.