

Title	"Aegis : the invisible war" : making of a multi-player board game about information security
Sub Title	
Author	张, 弛(Zhang, Chi (Nora)) Kunze, Kai
Publisher	慶應義塾大学大学院メディアデザイン研究科
Publication year	2017
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2017年度メディアデザイン学 第586号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40001001-00002017-0586

慶應義塾大学学術情報リポジトリ(KOARA)に掲載されているコンテンツの著作権は、それぞれの著作者、学会または出版社/発行者に帰属し、その権利は著作権法によって保護されています。引用にあたっては、著作権法を遵守してご利用ください。

The copyrights of content available on the KeiO Associated Repository of Academic resources (KOARA) belong to the respective authors, academic societies, or publishers/issuers, and these rights are protected by the Japanese Copyright Act. When quoting the content, please follow the Japanese copyright act.

Master's Thesis
Academic Year 2017

”Aegis: The Invisible War”: Making of a
Multi-player Board Game about Information
Security

Keio University Graduate School of Media Design

Chi (Nora) Zhang

A Master's Thesis
submitted to Keio University Graduate School of Media Design
in partial fulfillment of the requirements for the degree of
MASTER of Media Design

Chi (Nora) Zhang

Thesis Committee:

Associate Professor Kai Kunze	(Supervisor)
Professor Sam Furukawa	(Co-supervisor)
Professor Matthew Waldman	(Co-viewer)

Abstract of Master's Thesis of Academic Year 2017

”Aegis: The Invisible War”: Making of a Multi-player
Board Game about Information Security

Category: Design

Summary

Information security has been more at risk in recent years than before. In 2016, 4149 worldwide data breaches compromised more than 4.2 billion records. There is no doubt that information security has been prove to be among highest importance for any digitalized company. One element that cannot be neglected on the way of building stronger information security is raising information security awareness, as human error causes alarming rise of 93% of data breaches globally. However, lack of interests among the audience has been putting great challenges for information security training.

Aegis: The Invisible War is a multi-player card-based strategy board game designed with the purpose of intriguing interests and raising awareness in information security. The game sets in a corporate environment where players play as companies viciously competing with each other by attempting to attack opponents' information security and building up their own information security defense. Successful game play involves better strategies with players' own resource, fast re-planning according to opponents' actions and as always, a good luck. This thesis presents the final design of the game, as well as a record of iterations through ideation sessions and playtest sessions. Those sessions also have prove that the final design of ”Aegis: The Invisible War” is a fun game play experience that intrigue players' interests in information security.

Keywords:

Board Game, Game Design, Information Security, Strategy Board Game, Card-based Board Game

Keio University Graduate School of Media Design

Chi (Nora) Zhang

Acknowledgements

The development of this project is similar to bring up a child of my own. As the thesis goes through different stages of the child, I go through every stage of my life, and would like to express my gratitude for everyone who has given me love, support and strength. It is because of every one of you that I am who I am right now.

I would like to thank my parents, especially my mother, who have given her heart and soul into bring me up properly. I hope one day I would be able to repay you, mom. I love you from the bottom of my heart.

I would like to thank Professor Kai Kunze, who have guided me through KMD program. He has taught me to never stop learning.

I would like to thank Professor Sam Furukawa, who is so kind and generous, and always supportive of my passion.

I would like to thank Professor Matthew Waldman, who have helped me push the project forward tremendously over a short period of time.

I would like to thank George, who have stood by my side throughout the project and given me advice and suggestions, and most importantly companion.

I would like to thank CEMS program, my Business Project teammates, and all the colleagues during this one year. It is one year that I have changed the most, but also the one year that I have grown the most, the one year that defines me, who I am, and what I believe.

I would like to thank Dani, who offers me joy 24/7 and puts a smile on my face anytime of the day, and at the end of it all, makes me a better person.

I would like to thank Ploy, who shares my happiness, frustration and despair. It is my pleasure to have you by my side from beginning till end.

I would like to thank everyone who contributed to the process of this project. We have accomplished this, together.

Table of Contents

Acknowledgements	ii
1 Introduction	1
1.1 Background	1
1.2 Game Concept	2
1.3 Reasons & Hypothesis	2
1.4 Main Takeaways	3
1.5 Thesis Structure	4
2 Related Works	5
2.1 Information Security	5
2.1.1 Introduction	5
2.1.2 Information Security Awareness	7
2.2 Board Games	9
2.2.1 Entertainment & Serious Games	9
2.2.2 Strategy Board Games	9
2.2.3 Games about Information Security	10
2.3 Contribution of This Research	14
3 Aegis: The Invisible War	16
3.1 Concept Overview	16
3.1.1 Naming	16
3.1.2 Logo	17
3.1.3 Genre	17
3.1.4 Theme	18
3.1.5 Story	18
3.2 Purpose & Significance	18
3.3 Art Style	18
3.4 Target Audience	18
3.5 Game Elements	19

TABLE OF CONTENTS

3.5.1	Boards and Tokens	19
3.5.2	Rule Book	20
3.5.3	Cards	22
4	Game Development Journal	26
4.1	version 0.1.0: A Game about Information Security	26
4.1.1	Why Information Security	26
4.1.2	Inspiration	27
4.1.3	Reference Games	27
4.2	version 0.2.0: "The Guardian"	28
4.2.1	Concept Description	28
4.2.2	Ideation Sessions	29
4.2.3	Major Changes	30
4.3	version 1.0.0: "The Empires"	31
4.3.1	Concept Description	31
4.3.2	Playtest Sessions	39
4.3.3	Major Changes	41
4.4	version 1.1.0: "Empires v2.0"	41
4.4.1	Concept Description	41
4.4.2	Playtest Sessions	46
4.4.3	version 2.0.0: "Aegis: The Invisible War"	47
4.4.4	Evaluation	48
4.4.5	Main Takeaways	53
5	Conclusion	56
5.1	Concept Validation	56
5.2	Possible Improvements	57
5.3	Extension of Concept	57
	References	58
	Appendix	60
A	Card Lists	60
A.1	Attack Cards	60
A.2	Defense Cards	65
A.3	Event Cards	69
B	Card Decks	73

TABLE OF CONTENTS

B.1	Attack Cards	73
B.2	Defense Cards	75
B.3	Event Cards	78
C	Reference of Card Content	78
C.1	Attack Cards	78
C.2	Defense Cards	79
D	Pre-play Survey	81
E	Post-play Survey	84

List of Figures

2.1	Lack of interests is one of the challenges regarding information security awareness training. [9]	8
2.2	SECWEREWOLF: a role-play board game where players are assigned different roles in a cyber breach scenario.	11
2.3	An example of a web-based information security awareness training game.	11
2.4	Game of Threats: a digital board game designed by PwC to simulate an actual cyber breach, where players have to make quick, high impact decisions with minimal information.	12
2.5	Cyber Security Board: a board game designed by LAC to facilitate cyber security training among students.	12
2.6	Cyber Threat Defender: a multi-player collectible card game designed by CIAS, a cyber security program at UTSA (The University of Texas at San Antonio) to teach essential cyber security information and strategies.	13
2.7	Netrunner: a two-player Living Card Game set in a dystopian, cyberpunk future and pits a megacorporation and its massive resources against the subversive talents of an individualistic runner.	14
3.1	Logo and title of "Aegis: The Invisible War".	17
3.2	Player's board.	19
3.3	Public pool.	19
3.4	Round tracker.	20
3.5	Workers' tokens.	20
3.6	Basic Attack Card.	22
3.7	Attack Cards of different levels.	23
3.8	Sample Defense Card.	24
3.9	Sample Event Card.	25

LIST OF FIGURES

4.1	Above and Below: a mashup of town-building and storytelling where players compete to build the best village above and below ground.	28
4.2	The Guardian: game flow.	29
4.3	Ideation session with a game designer on November 11th, 2017. . .	30
4.4	First prototype of this project.	31
4.5	Example of the first prototype.	39
4.6	Playtest session for "The Empires" on November 24th, 2017. . .	40
4.7	Playtest session for "The Empires" on November 29th, 2017. . .	40
4.8	Second prototype of this project.	44
4.9	Sample cards of second prototype.	45
4.10	Playtest session for "Empires 2.0" on December 10th, 2017. . . .	46
4.11	Playtest session for "Empires 2.0" on December 13th, 2017. . . .	46
4.12	Playtest session for "Empires 2.0" on January 13th, 2018.	47
4.13	Complete design of Aegis: The Invisible War.	48
4.14	Pre-play survey result on interests of board game and information security.	49
4.15	Post-play survey result on if the theme fits the game mechanisms. . .	50
4.16	Pre-play survey result on information security awareness in private life.	50
4.17	Pre-play survey result on information security awareness in working environment.	50
4.18	Pre-play survey result on how often players play board game. . . .	51
4.19	Post-play survey result on first player advantage.	51
4.20	Post-play survey result on interaction.	52
4.21	Post-play survey result on interests.	52
4.22	Card design evolution.	54
B.1	Design of all Attack Cards.	73
B.2	Design of all Attack Cards.	74
B.3	Design of all Defense Cards.	75
B.4	Design of all Defense Cards.	76
B.5	Design of all Defense Cards.	77
B.6	Design of all Event Cards.	78
D.1	Pre-play survey.	81
D.2	Pre-play survey.	82

LIST OF FIGURES

E.1	Post-play survey.	84
E.2	Post-play survey.	85

List of Tables

4.1	List of Attack Cards created for the first prototype.	32
4.2	List of Defense Cards created for the first prototype.	35
4.3	List of Event Cards created for the second prototype.	42
A.1	List of Attack Cards.	60
A.2	List of Defense Cards	65
A.3	List of Event Cards	70

Chapter 1

Introduction

This chapter lays out the basic information of the project, introducing the background in short where the need for this project is stated, basic game concept where basic game play is explained, the reason why I started the project and some hypothesis made prior to the development process, and main academic takeaways from the project. This chapter serves as a foundation where further chapters build upon.

1.1 Background

Meet Stephanie. She is a information security consultant. Meaning? She gets hired by companies to hack into their own facilities. This time, she faces the challenge of fully secured buildings: armed guards, badge readers, biometric security controls and turnstiles at every entrance. Stephanie knows that she has to look from a different angle. She opens her computer and gets on LinkedIn. After a while of searching, she finds her target: Mary, newly-assigned assistant, with a public Facebook account. After figuring out Mary's whole life journey from her social media accounts and her passion for children and caring new moms, Stephanie picks up the phone and calls Mary, claiming to be a project coordinator introducing a designer to renovate the facilities. When Mary asks for documents that should be filed a while ago, Stephanie goes for her soft-spot, apologizing for missing the documents because of her maternity leave, which results in Mary's empathy and a long conversation about babies and parenting, and a scheduled meeting at the office with the designer. The next day, the designer Stephanie is warmly welcomed by Mary and her co-worker, given a visitor pass, and showed around the manufacturing floor, data center, office areas, etc. during lunch break. As the lunch break ends, the workers have to go back to work, while Stephanie still seems to be examining the floor. Having no doubt of Stephanie's true incentives, they kindly

leave Stephanie alone to her "work": access to every corner of the facilities.

Described above is a real-life story told by a physical penetration tester and information security consultant. According to her, the success of her social engineering hack could have been avoided at any step: if Mary calls the headquarter to verify Stephanie's request; if any of the employees asks her for an official ID; if the workers find someone else to escort her through the building... [5] In general, a higher information security awareness.

As cyber attacks grow stronger and bring more severe consequences in the recent few years, "information security" has become a hot topic among not only IT companies but also any corporation that has, is or will go through digitalization. Everybody knows that information security awareness is one of the keys to a stronger information security, but as of today, how to efficiently raise information security awareness remains unclear. This project offers one suggestion from an unique angle.

1.2 Game Concept

This project proposes the design of a multi-player card-based board game experience that will intrigue players' interests in the topic of information security. The game goes by the name of "Aegis: the Invisible War".

In this board game, players play as companies viciously competing against each other by attempting to attack others' information security and steal their information. Therefore, at the same time, players must build up their own information security defense to protect themselves from others' attacks. In order to conduct attack and defense actions, players must find best strategy to use their resources, which include workers and money. As players share the same public resource, they have to compete against each other in conducting better actions. The game play involve planning the best strategy using own resource, adjusting the plan according to other players' moves, and also having good luck with dice-throwing actions. In the end, victory belongs to the player who has the best strategy on attacks and defends.

1.3 Reasons & Hypothesis

The first inspiration came me during my Business Project in CEMS program. As a team we were asked to work on information security risks and mitigation

plans for companies facing Industry 4.0 in five years. Through the experience, I learned the importance of information security in a corporate environment. As much fun it was to work as a team, all the members, including me, were not too excited about the topic. Information security has not been viewed as one of the most interesting topics in the world. And it was not just us. During our discussion with Chief Security Officer of Nokia, we learned that making effective Information Security Awareness training has been a challenge, even for a company like Nokia. That was when this question came to my mind: how to make information security fun? Therefore, the main goal of this project is not to seriously educate people about information security, but to intrigue interests in the topic by casual game playing, which potentially could lead to better acceptance of future training.

As I do not have professional education in the field of information security or computer science, the focus of this project is not on the full creation of card content. A basic content will be conducted, but can be changed or expanded in the future when a team with experts is formed. The focus of the current project is on the creation of game play that serves the goal. Even though I do not have professional training on game play either, workable prototypes can be made with research on game design and iteration through play tests.

In relation to the experience of game play - Aegis: The Invisible War - a few hypothesis were established beforehand:

- the game should be fun and engaging to play.
- however, as it is a strategy board game, the game should be more enjoyable when players try their best to strategize.
- players should be more interested in the topic of information security after the game play.
- the game should be most effective to someone who is familiar with strategy board game. Based on that, players need to be patient in getting the rule.
- players should get better at the game the more they play, as they get more familiar with attack and defend techniques that are shown on the cards.

1.4 Main Takeaways

The main takeaways from this project derive from three process during the development: content preparation and creation, game play design and design creation.

- During the content preparation and creation process, abundant academic research in the field of information security, as well as hacking and social engineering was conducted. Later on when the content is being created, the result of the research was transferred to game content in combination with game play.
- During the game play design, I learned about basic game design theories and board game design fundamental. Based on these knowledge, a physical board game and its game play was designed accordingly to reflect the abstract concept of information security attacking and defending.
- During the design creation, I used different tools to create prototypes in different stages, from the most efficient to the most advanced. Storytelling was important in the latter stage of the project, adding the appeal of the game to its users. Same goes to brand design and marketing, as the development of the project starts to show great potential of hitting its targeted market.

1.5 Thesis Structure

This thesis is divided into 5 chapters. Following this introduction chapter, literature review and related works are analyzed regarding the topics of information security and board games, from which the thesis establishes the contribution of the game. Chapter 3 presents the complete concept of the final design of "Aegis: The Invisible War". The next chapter shows the development of the game design, from the initial idea to its current stage through several iterations, including the evaluation process and result of the final design. The last chapter concludes that the concept is valid, as well as suggests possible improvements and extension of the concept.

Chapter 2

Related Works

This chapter presents the academic research on information security and game design theories as well as related existing games conducted prior to the design and development of the actual board game. The result proves the existence of the problem that this project sets out to solve, as well as the lack of any existing product, service or platform serving the same purpose. Apart from that, these result lays the foundation where the actual game is built up, including the content and game play, which is a physical reflection of the abstract concept of these topics.

2.1 Information Security

This section presents the scale and scope of information attacks nowadays, and their severe consequences. It then lays out the current structure for a standard structure and dimensions of information security, which is later used during the game development stage as a source of content creation. It then reveals information security awareness as an important and fundamental element, and the problem existing in the current information security awareness training, which this project sets out to solve.

2.1.1 Introduction

As the number of information attacks increase as well as their financial and reputational impact on businesses of all industries, information security has become a familiar topic to many organizations. Alberts and Dorofee describe information security as determining what needs to be protected and why, what it needs to be protected from, and how to protect it for as long as it exists [2]. According to the 2016Data Breach QuickView report [13],4149 worldwide data breaches compromised more than 4.2 billion records in 2016. Aware of the amount and influence of information attacks, both academia and organizations have been conducting

research and developing practices to fully understand the mechanism of information security in order to develop an information security management system to be adopted throughout different industries.

Dating back as early as 1995, five main information security components have been identified: hardware (i.e. firewalls), software (i.e. encryption), data (i.e. classification), procedures (i.e. policy) and people (i.e. training). For each component, researchers have established a set of information security principles. These can be summarized along different dimensions outlined below [6]:

- **Confidentiality** refers to limiting the access to information only to authorized individuals. This task has proved to be increasingly difficult as the demand for a sharing information through fast-speed network and cloud storage grows, giving more access of more data to more people. The Internet Security Threat Report published by Symantec [16] shows that 25% of data in 2016 is broadly shared.
- **Integrity** refers to ensuring that the content of information is stored and processed correctly. It also involves how information is interpreted, whether it is presented correctly and processed fully. What it requires from the employees processing the information is not only numerical and language skills, but also the ability to read, present and comprehend information in a way that aligns with business strategy. Therefore, organizations not only need to secure the information, but also the interpretation of it.
- **Availability** refers to making sure that the information is accessible to the organization at any time needed. In general, authorized users expect information to be available at a given time and format. However, failure in availability can be commonly found in organizational practices. A typical example is a system breakdown. Others include denial-of-service incidents, referring to situations that prevent legitimate users from having reasonable access to the information [14].

As a fundamental concept in information security, the three dimensions mentioned above, commonly known as the CIA tripod, is a basic and starting step to protection of any information, and can be applied usually to any secured system. However, it has been suggested that the CIA triad is not enough. [3] Other factors besides the three facets of the CIA triad are also very important in certain scenarios. Here for this project, one concept can not be ignored:

- **Non-repudiation** refers to making sure that during a transaction of information, one party cannot deny having sent the information, nor having received the information. This ensures that actions of parties involved during the transaction of information is verified and authorized. An example of compromised non-repudiation can be an easily forgeable private key or digital signature, which results in the possibility of sender denying having sent the information, claiming that the authorization have been forged.

Based on the understanding of these dimensions, numerous researches and publications have developed a number of different models to ensure information security taking on various approaches. Recent discussions about information security have been focused on two trends: technology and human behavior. They mainly concern challenges brought by disruptive innovation and technologies, and new ways of human interaction in organizations. The discussion about new technologies all confirm the need of business to invest in leading technologies in order to survive in an increasingly competitive world. However, there is a general concern about the maturity of these technologies in terms of information security, and if organizations are actually ready for the implementation. Researches have revealed significant vulnerabilities of information security in IoT systems, blockchain technology and AI systems, as the security aspect of these technologies continue to be overlooked. Whats more, many companies are rushing into adopting advanced technologies without carefully planning and understanding related security concerns. However, more researches have stated that information security is not only limited to technological development, but also strongly connected to human behavior.

2.1.2 Information Security Awareness

As technical systems have to be operated and used by people, information security is no longer a technical problem, rather a social and organizational problem. Thomson and Von Solms [17] proposed that information security refers to a kind of behavior that can be learnt, proposing the term "Information Security Awareness". According to research, it is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee. Human error causes alarming rise of 93% of data breaches globally. [12] All of these research findings point to the importance of information security awareness.

Raising information security awareness can be based on formal and informal

sources, which can further be influenced by operational, physical, and technical actions within the computing-environment. Additionally, the cognition, behavioral intention, attitude, and affective responses of the individual user play a decisive role in shaping human behavior. Recent discussions about human behavior address concerns about lack of trust in a highly-cooperative business environment. In this environment, global borders have started to blur due to a lack of policies and practices to ensure supervision as false information gains instant credibility without verification. The lack of principles to be followed during human interaction concerning information security, such as responsibility, integrity, trust and ethicality, resulting in high risk stemming from privileged employees and espionage. This reveals the urgent need for organizations to work on people management in relation to information security, including identifying key principles, cultivating cooperate culture and developing policies throughout employment tenure.

Despite the urgent, information security awareness training has been proved to a quite challenging tasks. Not only is there a lack of academic research conducted on good practice of information security awareness training, it has also been proved that the current methods do not seem to be working at a level where they are meant to. In 2014, West Point ducted an experience sending phishing emails to cadets who have undergone 4 hours of security training. A surprising 90% of them still clicked on the embedded link. [1] One of the reasons might be quite obvious: boring (Figure 2.1).



Figure 2.1: Lack of interests is one of the challenges regarding information security awareness training. [9]

Employees finding information security training boring seems to be one of the challenging facing effective training results.

2.2 Board Games

In this section, basic game design theory and board game fundamentals are presented. The concept of a "serious game" or an "educational game" is also discussed. These discussions help forming the basic game concept and game design of this project. Then, a list of existing games about similar topic is discussed, indicating the market need of this project.

2.2.1 Entertainment & Serious Games

Nowadays, with the development of mobile phone technology, games have developed in multiple forms, platforms and genres. There are single-player, multi-player, massively multi-player games, and people play them on computers, consoles, hand-held devices, but also simply outside, in a play room, with cards, on boards, etc. Despite the variety of forms games can take, at the core of it is one word: playfulness. [15] Schell gives games a more detailed definition:

"A game is a problem-solving activity, approached with a playful attitude".

This already points to the possibility of combining educational value with entertainment purpose of games.

While the majority of games created up to today, no matter what form they take and what platform they target, are designed for entertainment, engagement and satisfaction, a great amount of researches have been trying to add educational purpose to game designs, and many games have been used as educational materials after modification if not as they are. Although, compared with standard teaching methods, empirical evidence for improved learning of declarative knowledge through game playing is ambivalent and suggests that it depends on other factors (e.g., facilitation skills), games are known to be effective in enhancing motivation and increasing student interest [4] [8]. In conclusion, a game could create a new, but easy to understand language for its players, which is rooted in common gaming experience and can serve as a starting point to introduce particular terminology necessary for an understanding of certain topic.

2.2.2 Strategy Board Games

Strategy games usually have a very important board and a narrative which drives the game's progress. These games often involve a heavy amount of co-op and

competitive play, forcing players to make and break alliances over the course of the game.

Players are usually participating as much in the game itself as they are in higher-level mind-games with each other: trying to get ahead, form alliances, and discern their opponent's motives. These games are generally marked by longer game sessions and are sometimes affectionately referred to as "friendship-ending games", because of how passionate players become. Among the most well-known games in this genre is Risk.

As one of the sub-genre of strategy board games, card-based strategy games are strategy games where cards are the primary game element. Games like this vary heavily, but there is often a drafting mechanic, or an element of character or base building where players use cards to gain abilities or bonuses. The goal in games like this can be based on victory points, trying to complete a specific set of cards, or eliminating certain target players, among others. Card-based strategy games usually has a central theme, separating themselves from games like Poker. Among the most well-known card-based strategy games is 7 Wonders.

2.2.3 Games about Information Security

Although there are many games that touch upon the topic of hacking, there are only a few that evolves around the experience of being a hacker. Among them, the most well-known games are Hacknet, Hacker Evolution, Watch Dogs, and Hackers. There are even fewer games that look on the other side of the interaction: defending attacks and building up security. There is a role-play board game called SECWEREWOLF developed by Japan Network Security Association where players are assigned different roles and play verbally with a plot facilitator.



Figure 2.2: SECWEREWOLF: a role-play board game where players are assigned different roles in a cyber breach scenario.

There are also a number of web-based games made for information security training. However, they appear to be scenario-specific and text-heavy.



Figure 2.3: An example of a web-based information security awareness training game.

Attempts have been made to create a board game in the field. Here are a list of these games.

- PwC: Game of Threats

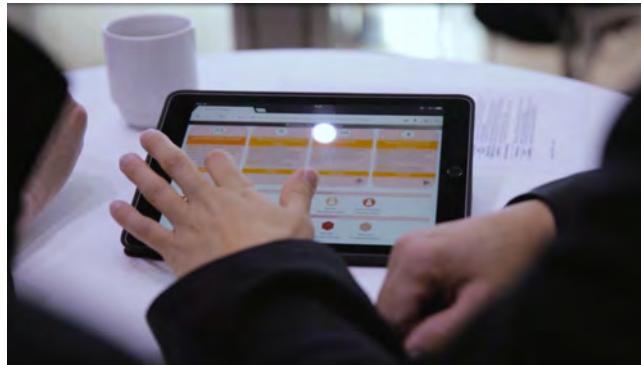


Figure 2.4: Game of Threats: a digital board game designed by PwC to simulate an actual cyber breach, where players have to make quick, high impact decisions with minimal information.

As presented, this product is a digital board game, which results in a game play experience quite different from a physical board game. Also, each side is limited to only one kind of experience, either attacking or defending. It is text-heavy, and needs to be played with a PwC moderator.

- LAC: Cyber Security Board



Figure 2.5: Cyber Security Board: a board game designed by LAC to facilitate cyber security training among students.

This board game is developed with a specific purpose as a assisting tool during cyber security workshops. It only concerns cyber attacks, played by multiple groups and is quite complex. Therefore, it is played with a company facilitator explaining the content and game play. Same as "Game of Threats", it is not designed for the general board game market. There

are a number of board games designed by other cyber security companies as a tool during cyber security workshops and trainings: Kaspersky Industrial Protection Simulation designed by MHPS, Incident Simulation Boardgame by TrendMicro, etc. However, they all only allow players to experience one side of the actions, need to be played with facilitators and with text-heavy content and complex game play not suitable for the general board game market.

- Cyber Threat Defender

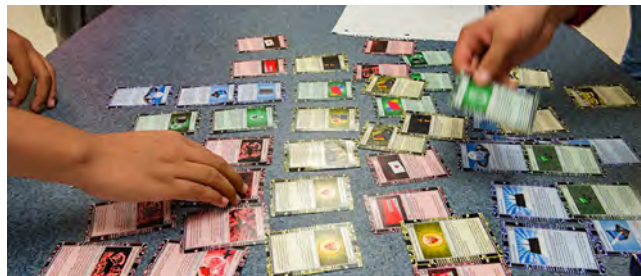


Figure 2.6: Cyber Threat Defender: a multi-player collectible card game designed by CIAS, a cyber security program at UTSA (The University of Texas at San Antonio) to teach essential cyber security information and strategies.

This game is most similar to the game of this project. It contains different types of cards that may result in attack or defend based on the game play, and offer players points when succeed. This game does let players experience of attacking and defending, however it is also only limited in cyber attacks and defend, and the only element that players have to compete and strategize is the cards. This results in the game being a more serious and educational game. It is currently being used in classrooms across USA.

As discussed before, most of them are developed as a tool for workshops of cyber security, and only serve as an educational purpose and are played with the present of a facilitator. The only card-based strategy board game that is released to the market and has been quite successful is Netrunner.

- Netrunner



Figure 2.7: Netrunner: a two-player Living Card Game set in a dystopian, cyberpunk future and pits a megacorporation and its massive resources against the subversive talents of an individualistic runner.

However, even though the game has been largely embraced by players all over the world for its dynamic game play and intriguing story telling, its futuristic game setting drives away from the purpose of information security awareness despite a few game actions related to cyber attacks and defend.

Based the research and discussion presented above, there has not been a card-based board game produced currently that is released to the general board game market, not limited to the purpose of security awareness training and can be played without a facilitator, covers the complex dimension of information security, offers players experience of both attacks and defend, and contains multiple game elements. This marks the uniqueness of Aegis: The Invisible War.

2.3 Contribution of This Research

In conclusion from literature review on topics of information security and board games, this thesis states the problem that this project aims to solve: as important as it is to raise information security awareness, effective training has been

challenging due to lack of interests from the audience. Games, with its playful nature, could be a useful tool in intriguing interests. As a card-based board game suitable for general board game market that involves both attacks and defense of information security has yet to be made, Aegis: The Invisible War offers a unique solution to the problem.

Chapter 3

Aegis: The Invisible War

This chapter presents the final design of this project: Aegis: The Invisible War in detail, from the background story to its game elements. The way to present the final design is based on Game Design Document theory. [11] It is referred to as a living document that records the constantly updating development of a game project. Although there is a general guidance on what topics should be included in a Game Design Document, there is no fixed rules on what to include, as each projects have different needs and focuses. Therefore, it is up to the developer what to include and what to leave out. Here, related topics have been selected, which include concept overview, purpose & significance, art style, target audience, game elements, rule book and cards.

3.1 Concept Overview

3.1.1 Naming

The current naming of the game, Aegis: The Invisible War, defines the overall atmosphere, tone, and style of the game. Aegis origins from Greek mythology. It is commonly interpreted as a shield carried by Athena, the goddess of wisdom and military victory, and her father Zeus. The symbolism of Aegis and its connection to Athena indicates the focus of the game lies in defense and guard, leading to victory. "The Invisible War" indicates the digital nature of the interaction between attacks and defends of information security. Together, the title sets a mysterious, competitive, and tough emotional tone for the game.

3.1.2 Logo



Figure 3.1: Logo and title of "Aegis: The Invisible War".

The logo here sets the overall style of graphic design: flat icons. It is the style that is generally used not only in board games, but also in business presentations. Therefore, it creates a sense of familiarity among the players. The image of shield once again emphasizes on the topic of information security, which is the main theme of the game. The swords refers to the part "The Invisible War" in the title, which conveys the competitiveness of the game and the nature of information security. The color is set to a light shade of sapphire blue (Hex triplet: 00addc), that conveys concept of calm, secure, and protected. The font is set to Flexo Caps, which is a demo font that can be used freely. This font is chosen for its square shapes convey a secured and safe image, while the smooth lines keep it fun and pop.

3.1.3 Genre

Aegis: The Invisible War is a card-based strategy board game. It can be played from 2 players to 4 players. The card decks can be expanded. A typical game play should be 20-40 minutes long.

3.1.4 Theme

The game is set in a corporate environment and evolves around topics of information security, hacking and defending.

3.1.5 Story

In the digitalized era, the battlefield of the invisible war is everywhere. You, CEO of an uprising IT company, faces vicious attacks from your competitors. They are trying to break down your security system and steal your vital information. You must use all the resources you have to protect your company from those attacks. At the same time, you may build hacking army of your own. The future of your company lies in your hands.

3.2 Purpose & Significance

The aim of this game is to intrigue players' interests in the topic of information security, raise information security awareness and potentially learn about basic attack and defend techniques of information security. As a result, players will be more interested in the topic, which can potentially lead to curiosity and self-learning, as well as better acceptance of future training.

3.3 Art Style

A consistent art style, which consists of flat icon graphics and Flexo Caps, is deployed to create a brand image: mysterious and intense, secure and safe, yet trendy and playful. It increases the attractiveness of the game and makes the players more engaged.

3.4 Target Audience

Targeted at gamers, board game fans and enthusiasts on a global base, the game is made for general board game market. It can be used for internal information security training in a corporate environment, but the game itself is enjoyable by anyone, regardless of their educational background.

3.5 Game Elements

4 Player's Boards, 1 Public Recourse Board, 1 Round Tracker, Workers (Hackers, Guards, Employees), Rule Book, Cards

3.5.1 Boards and Tokens



Figure 3.2: Player's board.

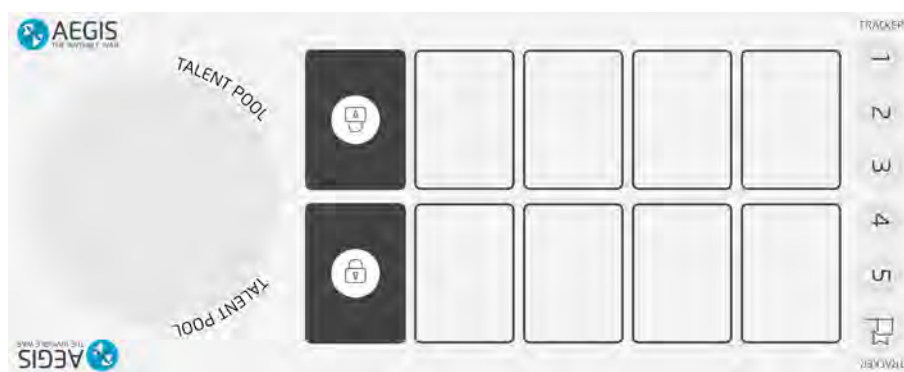
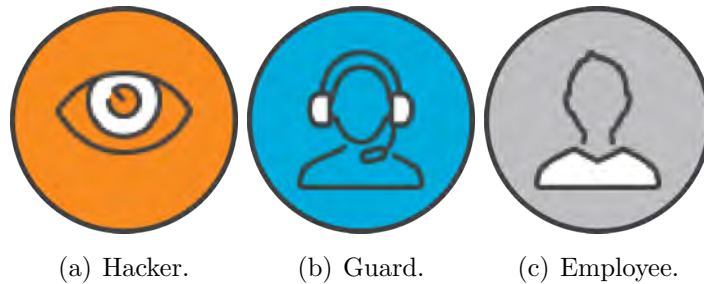


Figure 3.3: Public pool.



Figure 3.4: Round tracker.



(a) Hacker.

(b) Guard.

(c) Employee.

Figure 3.5: Workers' tokens.

3.5.2 Rule Book

Setting up

Every player gets 3 Employees, 2 Hackers, 2 Guards, 20 Coins.

Open 4 Defense Card, 4 Attack Cards for Card Pool.

Put 3 Employees, 2 Hackers, 2 Guards for Talent Pool.

Start a Round

Players decide who starts in the first round, then take turns to start the round.

- 1) Place round tracker.
- 2) Every player receives 5 Coins.
- 3) Return worker in the Training Area to Working Area, and Working Area to Lounge Area.
- 4) Open 4 new Defense & Attack cards.
- 5) Place 3 Employees, 2 Hackers, 2 Guards in Talent Pool.
- 6) Check if any workers should be occupied with continuing Effect.
- 7) Round starter Opens an Event card. After reading the description of the card,

player decides whether to activate the card and who to attack. If the player decides to activate the card, the player must accept the consequence. If the player decides not to activate the card, the card will be discarded.

8) Discard cards from the player's hand if needed.

During a Round

Players take turn to make one action.

Players can 1) hire worker from Talent Pool; 2) Send worker to work; 3) activate cards.

1) Pay 3 Coins for an Employee, 5 Coins for Hacker & Guard. Newly hired workers cannot be used for this round. Place them in the Working Area.

2) Send a worker to Training Area. The worker earns money for you that will be given at the end of the round. However, The worker will only be moved to the working area next round, which will make it unavailable for any other action. An employee earns 1 Coins; Hacker & Guard earns 3 Coins.

3) Activate the cards in your hand, or from the public Card Pool.

To activate a Defense card, pay the price, and place it by your side. For a Defense card to counter an Attack, it must already be activated prior to the Attack.

To activate an Attack card, you must fulfill the requirement, pay the price, and place it by your side. Your target must suffer the effect.

If one does not have enough workers, one must pay the amount of Coin for the workers. If one does not have enough Coin, one goes into minus. However, when money is minus, the player cannot purchase any card that costs money or hire any worker.

Throughout the turn, the player is allowed to draw one card from Attack card deck, and one card from Defend card deck.

The Round ends when no player can make any action.

End the Game

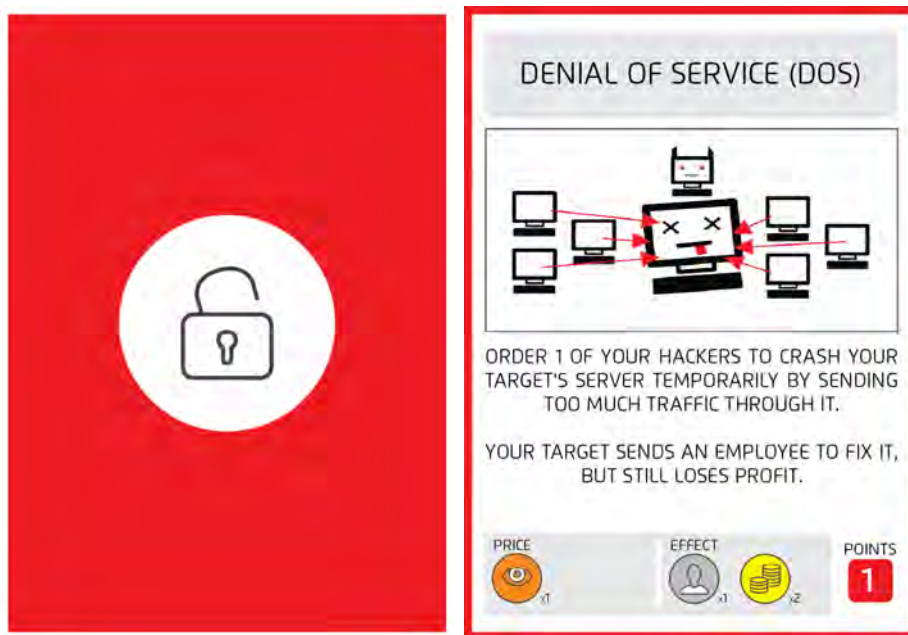
Count the points from all activated cards, both Attack & Defend Cards.

Whoever has more points win.

3.5.3 Cards

Attack Cards

A typical Attack Card contains five parts: title, description, price, effect and points. Title is the name of the attack, while the description gives a detailed use case of such attack with an image. Within the description, players will find reasons for the price and effect. Once a player decides to activate the card and pays the price, the target has to suffer the effect. The player will get the corresponding points.



(a) Back of Attack Cards.

(b) Sample Attack Card.

Figure 3.6: Basic Attack Card.

There are different levels of the cards. Some cards can be activated without any further requirement, while some cards require the player to have other cards activated as a base. Requirement is stated in the description session and marked in red so it is easy to spot.



(a) Base Attack Card.

(b) Attack Card that requires possession of another card.

Figure 3.7: Attack Cards of different levels.

The content of the card deck is created based on a number of online articles, journals and books. One of the most referenced book is Hacking: The Art of Exploitation by Jon Erickson [7]. The list of references used when creating the content will be listed in Appendix C, together with the ones used for Defense Cards.

Defense Cards

A typical Defense Card contains similar elements as a typical Attack Card. For Defense Cards, its effects are mainly protecting players from certain Attack Cards.

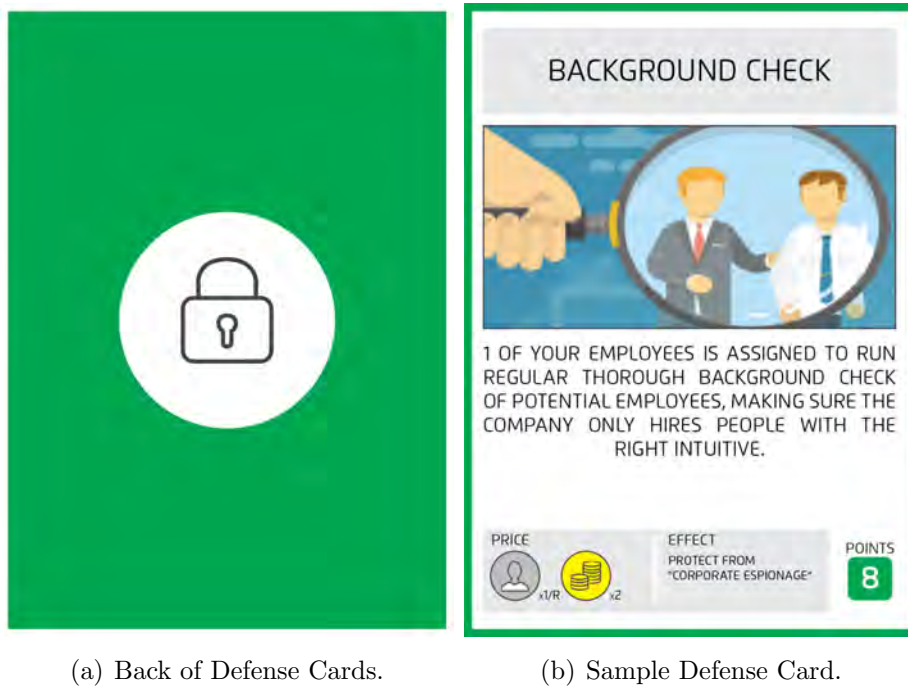


Figure 3.8: Sample Defense Card.

However, not every Attack Card can be defended. The example Attack Card in the previous session (Figure 3.6(b)), for example, can not be defended by a specific card.

Defending from Attack Cards is not the only function of Defense Cards. Effects of Defense Cards vary from increasing the result of dice throwing to disarming target's hackers.

Same as Attack Cards, the content of Defense Card deck is created based on a number of online articles, journals and books. One of the most referenced material is The Standard of Good Practice for Information Security 2016 created by Information Security Forum [10]. The list of references used can be found in Appendix C following the ones of Attack Cards.

Event Card

An Event Card consists of title, description, and consequences. There are a success consequence and a failure consequence. The result is decided by the result of dice throwing. The player has to throw the dice twice. If each of them is equal or more

than the printed number on the card, adopt success consequence and target has to suffer the indicated effect. Otherwise, adopt failure consequence and player has to suffer the indicated effect.



(a) Back of Event Cards.

(b) Sample Event Card.

Figure 3.9: Sample Event Card.

Chapter 4

Game Development Journal

The creation of this game to me has been a long and weary journey. There has been lots of dead ends, circling around and getting lost. However, every step, no matter how frustrating it made me feel at that time, is equally valuable to the overall project. This chapter can be seen as a journal, a record of how this project develops from just an idea to its current stage. At the end of this journey, I have summarized the main takeaways from this journey, as a record of self-growth, but also can be seen as the contribution of this project.

4.1 version 0.1.0: A Game about Information Security

4.1.1 Why Information Security

When I presented this project to people during the time I have been working on it, I got asked a lot of times: "But why did you choose to work on information security?" As a Media Design Master's student with a literature background, I am no way labeled as a tech savy, or someone who would be interested in the topic. However, it is this kind of reaction that proves further the significance of this project: information security should be a topic that everyone pays attention to.

I first encountered the topic when I started working as a team on a Business Project, where we were asked to analyze information security risks and develop mitigation plan for companies facing Industry 4.0 in five years. We were partnered with Nokia to work on this project. Despite the fun and achievement working with the team members, as well as the importance of information security for individuals and companies, we did all joke about what a boring topic it was. Soon we learnt that we were not alone. During an interview with Chief Security

Officer of Nokia, he told us that every quarter he has to make a slide deck and word document about information security practices and sent them to every employee in the company. However, he sadly realized that barely anyone read them through. This is when I realized that lack of interests has been creating huge challenges to efficient information security awareness training. I started asking a question: how can we make information security fun?

Although I am not a gamer of any sort, I do enjoy playing board games with friends a lot. From my experience, it not only offers entertainment, but opportunities to socialize, stimulate communication and deepen friendship. More importantly, it gets you interested in the theme of the game. That's when the idea hits me: a board game about information security that can be used for information security awareness training.

Just like that, the journey begins.

4.1.2 Inspiration

The inspiration of the game was stimulated by discussions and conversations with my team of the Business Project, as well as brainstorm sessions with another Business Project team that was working on the same topic. I have got approval from other team members to further develop the idea and try to realize it with this project. However, it would not have been possible to conduct this project without their input in the idea and their approval for me to continue working on it.

4.1.3 Reference Games

The mechanism of Aegis: The Invisible Game is much inspired by several board games that I enjoy playing. One of the most significant board games is Above and Below.



Figure 4.1: Above and Below: a mashup of town-building and storytelling where players compete to build the best village above and below ground.

Above and Below combines game plays from different genres of board games, offering a gaming experience to another level. During the game, players can experience crazy adventures when their choices and luck can change the happenings completely. They also need to strategise with different recourses they have, including villagers, houses that offer beds for villagers to rest, and caves that offer opportunities to go on adventures. As players are purchasing from a shared resource pool, they also have to change their plans according to the actions of their opponents.

With several brainstorm sessions and study about game design, the first stage of the project was born.

4.2 version 0.2.0: "The Guardian"

4.2.1 Concept Description

The project had a different name at this stage: "The Guardian". It also has a completely different setting.

First of all, it was a two-player board game, where one plays as a hacker, and the other plays as a guard. Both sides will have same recourse to start with, which includes money, human recourse, and guard/hack coins. During the game, both sides take turn to make actions. Both can either use money to hire people, or use both to human recourse to earn money, or use both to purchase guard cards. The

cards will give different effects, from simply increase recourse, or special guard techniques, such as educating your HR, which will increase the point of each HR counts at the end of the round.

The game ends when the hacker decides to hack. Then, players will reveal their hack/guard points. Hack/guard points come from free human recourse, guard coins, and certain cards. Just like reality where both hacking and defending combine with random possibility, both points will be added with the result of a dice. If the hacker has higher points than the guard, the hacker wins.

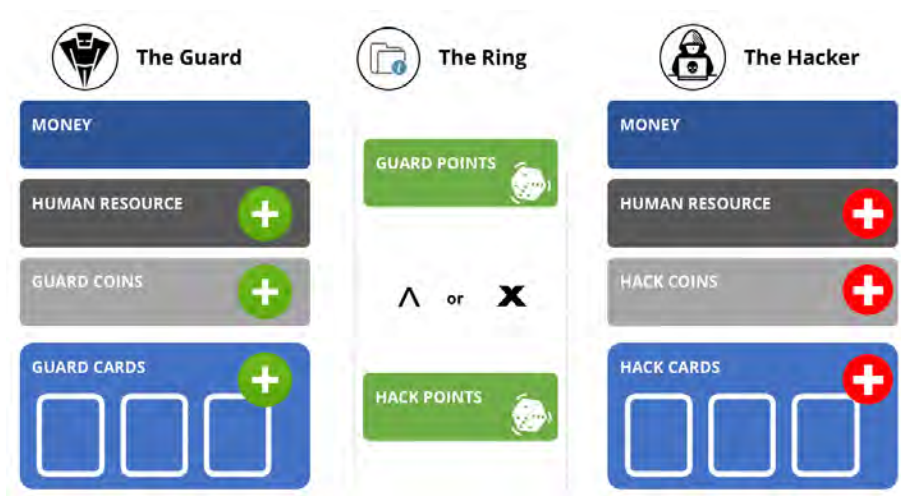


Figure 4.2: The Guardian: game flow.

4.2.2 Ideation Sessions

This idea is tested and evaluated during 3 ideation sessions with game designers as well as 2 interviews with information security experts.



Figure 4.3: Ideation session with a game designer on November 11th, 2017.

As this is the initial idea, it is expected that feedback is mostly suggestive. While the participants recognize the value of the concept, and the interviewees offer valuable suggestions on the card content (Bitcoin, block chain technology, social engineering, etc.), they indicate that there is huge room for improvement. Firstly, as the players build their actions from separate decks using their own resource, there is very little interaction between players. The only interaction happens at the end of the game, when the hacker decides to hack. This goes against the purpose of board game. Because of that, on another issue, the game will end very soon as it is completely in the hand of the hacker. Actions are limited from both sides. Finally, concept of winning not clear for the guard. If the hacker has higher points than the guard, the hacker successfully steals the guard's information and wins the game. However, if the guard has equal or higher points, he protects his information, which in reality means nothing happens. There needs to be stronger stimulation of victory for both players.

4.2.3 Major Changes

Based on the feedback, the project has gone through some major changes. Instead of one player attacking and one player defending, one player can play both sides. The concept of public resource shared by players is created to stimulate more interaction. This marks the beginning of version 1.0.0.

4.3 version 1.0.0: "The Empires"

4.3.1 Concept Description

This stage of the project was again labeled as a different name: "The Empires". One of the most important elements created during this stage is a storyline.

In the world of THE EMPIRES, companies are viciously competing with each other, by attempting to steal others information. Each player takes charge of a company. While attempting to attack others, one has to build up defense system to protect themselves too. Let the invisible war begin!

Based on the storyline, the basic game flow is created. Both players have same amount of recourse to start with (workers and money). They take turns to start the round. During each turn, one can hire more people, train their workers into hacker or guard, use workers and money to purchase cards. At the end of each round, players gain money from free workers and a certain amount of regular income. There are 6 rounds in total. At the end of the sixth round, players count the points from both Attack Cards and Defense Cards. Whoever has higher points wins.

First prototype is then created for the purpose of playtests.

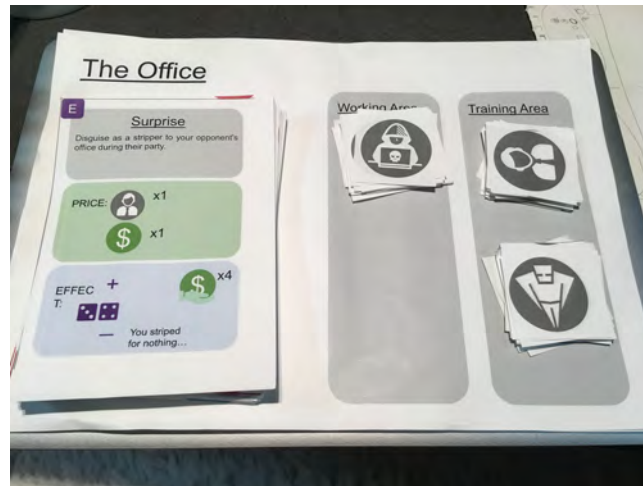


Figure 4.4: First prototype of this project.

At this stage, a basic card deck is created based on a number of online articles, journals and books of hacking and information security. The reference is listed in Appendix C.

Following are the lists of Attack Cards and Defense Cards created at this stage.

Table 4.1: List of Attack Cards created for the first prototype.

Name	Description	Price	Effect	Points
Denial of Service	Shut down the opponent's website	1 Hacker to work	-2 bits, 1 Employee to work	2
Corporate Espionage	Send an undercover to the opponent's organization	Lose 1 Hacker permanently, 1 Employee, 2 Bits	Gain 3 Bits from opponent each round, gain 1 Employee	7
Sticky Fingers	Approach one of the opponent's employees at a bar and steal the ID card	1 Hacker to work, 2 Bits	-1 Bit, 1 Employee to work	2
Route Hijacking	Hacking wifi router & gain access to the information being transmit through it	1 Hacker to work, 2 Bits	-5 Bits	5
MITM	Alter information transmit through the router, so your opponents' employees are receiving false information	1 Hacker to work, 2 Bits	-7 Bits	10
Pass	Steal the password by getting close with your opponent's and go through their notes	1 Hacker to work, 1 Bits	No effect when used alone	2
To the Cloud	Connect to the server of your opponent via the router	2 Hacker to work, 4 Bits	Gain 5 Bits from opponent	15

Continued on next page

Table 4.1 – continued from previous page

Name	Description	Price	Effect	Points
Takeover	Hijack your opponent's manufacturing control center	1 Hacker and 1 Employee to work, 3 Bits	-7 Bits, 1 Employee, 1 Guard to work	10
Microscope	Purchase a scanning software for your opponent's system vulnerabilities	1 Employee to work, 3 Bit	No effect when used alone	2
Bribe	Offer money to a employee of your opponent and get vital company secrets	1 Employee to work, 8 Bits	-10 Bits	10
Blackout	Cut down electricity cables and shut down your opponent's electricity supply	1 Hacker and 1 Employee to work, 3 Bits	-1 Employee, -2 Bits	2
No Connection	Cut down Internet cables and shut down your opponent's Internet connection	1 Hacker and 1 Employee to work, 3 Bits	-1 Guard and 1 Employee, -3 Bits	3
I see you	Hack into your opponent's security camera system	1 Hacker to work, 1 Bits	Plus 1 Dice Point for "Ninja"	1
Rerouting	Mess up with the router setting and shut down your opponent's Internet connection	1 Hacker to work, 3 Bits	-1 Guard and 1 Employee, -3 Bits	2

Continued on next page

Table 4.1 – continued from previous page

Name	Description	Price	Effect	Points
Ransom-ware	Infect opponent with ransom-ware, encrypt opponent's files, and ask for ransom	1 Hacker and 1 Employee to work, 3 Bits	1 Employee and 1 Guard to work, Gain 7 Bits from opponent	5
Fake News	Spread fake news that harm your opponent's reputation online	1 Employee to work, 2 Bits	-4 Bits	1
Implant	Get access to your opponent's database and alter information that leads to false prediction and analytics	2 Hackers to work	-4 Bits	7
Go Around	Hack the cloud database and leak your opponent's customers' confidential information online	2 Hackers and 1 Employee to work	-7 Bits	8
Hacking 4.0	Hack into your opponent's IoT device	1 Hacker	No effect when used alone	1
Acting	Contact your opponent's manager as a floor designer, ask for a office tour, enter the building and witness company secrets	1 Hacker to work, 1 Bits	Gain 5 Bits from opponent	8

Table 4.2: List of Defense Cards created for the first prototype.

Name	Description	Price	Effect	Points
Background Check	Regular thorough background check of potential employees, making sure the company only hires people with the right intuitive	1 Employee to work each round, 2 Bits	Deactivate "Spy"	8
Security Guard	Hire a security guard that checks your employees' identity during working hours	1 Employee to work each round, 2 Bits	Deactivate "Sticky Fingers"	2
Security Gate	Install a scanner at the entrance of your company building	1 Guard, 2 Bits	Deactivate "Sticky Fingers"	2
Touch ID	Install a biometric security system, that requires fingerprint recognition when your employees enter	4 Bits	Deactivate "Sticky Fingers"	2
Coded	All your information is sent with encryption	1 Guard and 1 Employee, 2 Bits	Deactivate "MITM"	5
Arm Up	Invest on better network infrastructure: stronger router system	1 Guard to work each round, 4 Bits	Deactivate "Leech"	5
Chameleon	System requires your employees to change their passwords every month	1 Guard	Deactivate "Pass"	2
Cloud Nine	The server you use is highly secured, guarded and encrypted	2 Guard, 6 Bits	Deactivate "Access to the Cloud"	10

Continued on next page

Table 4.2 – continued from previous page

Name	Description	Price	Effect	Points
Bayesian Filtering	Install an advanced filtering software that detects vicious emails for all incoming emails	1 Guard, 2 Bits	+1 on the dice result for Phishing	2
Classroom	Hold Information Security training class for all Employees	1 Guard, 2 Bits	+1 on the dice result for Phishing, Surprise	1/Employee
Double Spy	Turn the spy sent from the opponent against them by giving him more money than your opponent	2 Employee to work each round, 6 Bits	Gain 2 Bits from opponent each round	10
Justice	Trace back the IP address and report to the authority	1 Guard each round	Can be used once each round. If succeed, the attacker permanently loses a Hacker	4
The Head	Hire a Chief Information Security Officer	4 Bits each round	-1 all dice results of attacks	8

Continued on next page

Table 4.2 – continued from previous page

Name	Description	Price	Effect	Points
Know yourself	Purchase a scanning software for your system that reveal vulnerabilities	1 Guard, 1 Employee to work each round, 3 Bits	Deactivate "Microscope"	4
Firewall	Deploy an advanced Firewall: a computer in between all connection	1 Guard, 4 Bits	Deactivate "Implant", "To the Cloud"	6
Update Armer	Update Hardware devices connected to your network	1 Employee to work each round, 4 Bits	Deactivate "I see you", "Hacking 4.0"	5
All roads lead to Rome	Set up parallel network system for less protected devices: IoT, cameras, etc.	1 Guard	Deactivate "I see you", "Hacking 4.0"	3
Help	Hire a security company to protect your employees	2 Bits each round	+1 all dice results related to physical harm of your employees	4
Trust-but-verify	Establish verification process for actions that will endanger vital information	1 Guard, 2 Bits	Deactivate "Acting", +1 on the dice result for Surprise	8

Continued on next page

Table 4.2 – continued from previous page

Name	Description	Price	Effect	Points
PR	Establish PR department to monitor and deal with fake rumors fast and efficient	2 Employee to work each round	Deactivate "Rumor"	5
Block-chain	Ensure data integrity by introducing block-chain	2 Guard each round	Deactivate "Implant"	8
Partner	Choose your cloud provider wisely	2 Employee to work, 2 Bits	Deactivate "Go Around"	5
UPS	Establish a backup electricity power supply	3 Bits	Deactivate "Black-out"	3
Stay Connected	Establish a backup of your Internet connection	3 Bits	Deactivate "No Connection"	3
Backup	Backup all your information in a remote and secured location	1 Employee, 3 Bits	Deactivate "Flood"	3

At this stage, the prototype was made using the most efficient tool: Microsoft Powerpoint. Its easy-to-use system offers the shortest production time. As the purpose of playtest at this stage is mainly focusing on playability and the design needed to be changed later, this is the most reasonable choice of tool.



Figure 4.5: Example of the first prototype.

4.3.2 Playtest Sessions

Before the playtest during the creation of the first prototype, two more ideation sessions with 3 CEMS students and 1 KMD student were carried out to test if the basic game flow makes sense. Feedback includes making it into a multi-player games, balancing the effect of Defense Card and Attack Cards. Based on these feedback, a few changes on the game play were made: one can only draw limited amount of time from closed decks, and Defense Card has to be activated before Attacks.

After the ideation sessions, 6 playtest sessions were conducted with 9 players, including 6 KMD students, 1 CEMS student, 1 game designer and 1 MNC employee.



Figure 4.6: Playtest session for "The Empires" on November 24th, 2017.

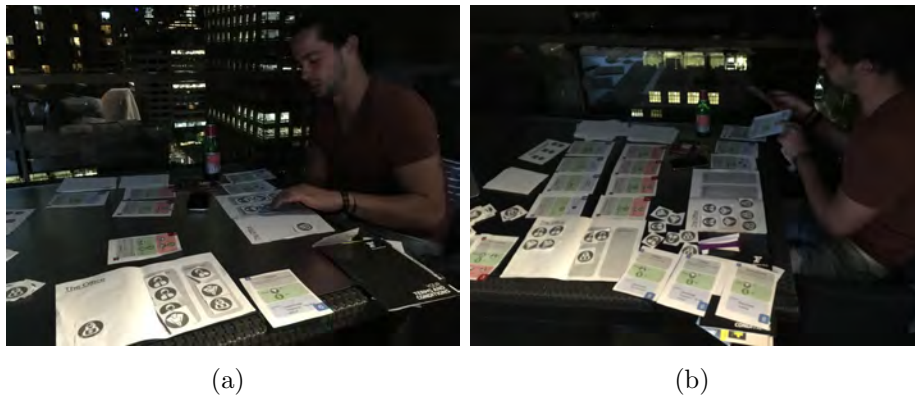


Figure 4.7: Playtest session for "The Empires" on November 29th, 2017.

Feedback

At this stage, feedback is qualitative, as the main focus is on the playability and improving the game play. It is taken in the form of interviews, observation and discussion. All players were interviewed before and after the gameplay about their education background, interests and previous experience in board game, interests and previous experience in information security before the game play. After the game play, players reflected on their game play experience. Already at this stage, players reported that game play itself is engaging and fun. However, some of the rules are still unclear or too complex, which interferes with a full enjoyment of the game play. 4 out of 5 players reported that they did get more interested in the topic of information security, as they remembered some new terms, the fact that

most attacks can be prevented if one is equipped with a defense, and the cards that made a great impact on the game play.

However, the feedback from the players also suggest a large room for improvement. Some rules got in the way of a fun game play experience. First player overpowers too much, as the first player can cast a lot of damage on the target. Some cards are too strong and the price, effect and points do not match. There is still a lack of interaction as one player takes too long to finish his turn. In the meantime, the other player has nothing to do. A problem is revealed that sometimes a player can not pay for the effect.

At this stage, one major problem is reported: players get so competitive and engaged in the game play that they focus too much on the price and effect but not the content about information security of the cards. When the cards have certain requirements on it, it encourages people to read. However, most of the cards can be played without reading about information security.

4.3.3 Major Changes

To improve the game play, a few adjustments need to be made. Considerations include adjusting the recourses to start with, thus limiting the impact from the first player, etc. To engage players more in the content of information security, consideration of adding images to the cards and more storyline to the content is proposed.

4.4 version 1.1.0: "Empires v2.0"

4.4.1 Concept Description

This marks a second version of the "Empires" stage. Changes on the card content are made to improve the storytelling, price, effect and points are adjusted to balance each other, and images are added to all cards.

Events Card

A deck of Events Card is created. This is to add more element of luck and fun in the game and show that sometimes information security can be endangered by random events or natural causes.

Table 4.3: List of Event Cards created for the second prototype.

Name	Description	Dices	Lost	Success
Phising	Send an email that contains a virus to all employees of your opponent	3,4	No effect	You gain one attack points of each Employee your opponent has
Witch	Deliver a overdue pizza to your opponent's office	4,5	You lose 5 Bits and 1 Employee permanently	Your opponent loses 4 Employees this round
Blackmail	Kidnap an employee and blackmail your opponent with vital company secrets	4,5	You lose 10 Bits and 3 Employee permanently	You gain 10 Bits from your opponent and your opponent loses 1 Employee permanently
Fire	Set your opponent's building on fire at night	4,5	You lose 8 Bits and 1 Employee permanently	Your opponent loses 14 Bits and 3 Employees to work
Surprise	Disguise as a stripper to your opponent's office during their party	2,3	No effect	You gain 4 Bits from your opponent
Secret Path	Dig a tunnel to your opponent's basement and steal their server physically	2,3	No effect	You gain 4 Bits from your opponent
Flood	A flood destroy your data center	4,5	You lose 6 Bits	no effect

Continued on next page

Table 4.3 – continued from previous page

Name	Description	Dices	Lost	Success
Damn those squirrels	Squirrels eating cables	3,4	You lose 4 Bits	or no effect
Ninja	Sneak in the building & get access to the server that contains vital company secrets of your opponent	4,5	You lose 1 Hacker permanently and -7 bits	Gain 4 Bits from opponent

Changes of Rule Book

The possibility of "training current Employee into Hacker or Guard" is eliminated, as it does not make sense in reality. The rule when player cannot afford the effect is made: when the player cannot afford to pay Coins, the player goes to minus. When a player has minus money, the player cannot purchase any card that costs money or purchase any worker. When the player cannot afford worker, the player must pay the price for the designated worker. One major change of the rule made at this stage is instead of one player making all the actions during one turn, players take turn to make actions. This is way more similar to information security attacking and defending in real life. It also balanced the waiting time and improved interaction among players, which is later proved by survey result.

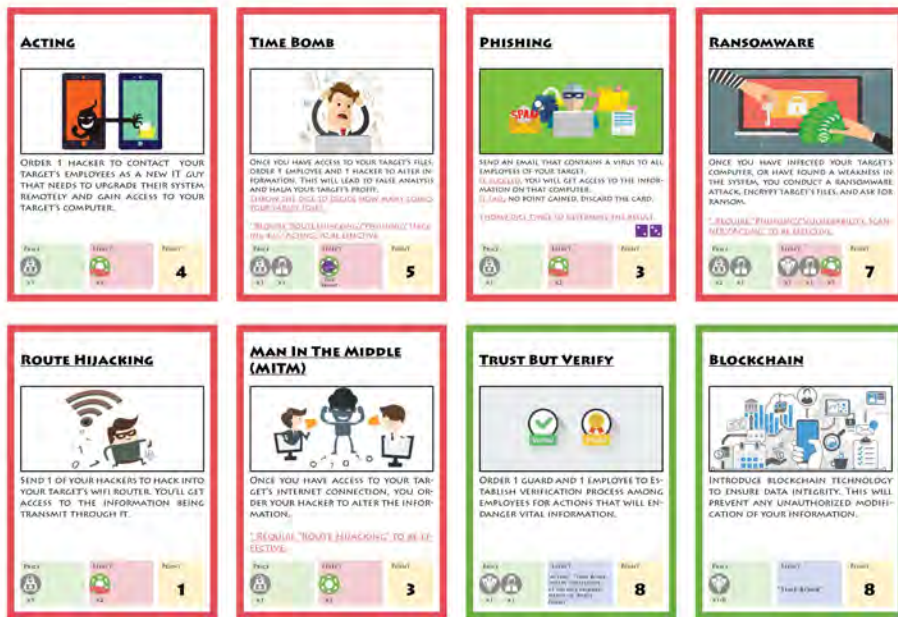
Second Prototype

At this stage, a second prototype was produced, where all cards have an image on it. This way, even if players do not read through the texts or cannot remember the content, the images will make an association with the title, leaving a stronger impact on the players about information security. With more design needed, the second prototype was made using Adobe InDesign.

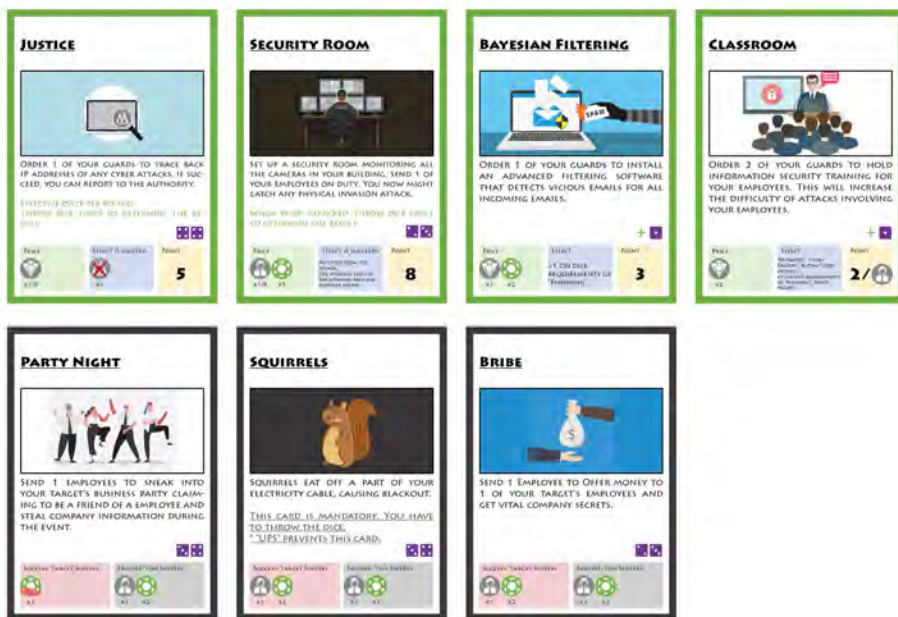


Figure 4.8: Second prototype of this project.

While making the cards, I also adjusted the balance of price, effect and points. One major change is all Defense Cards now offer more points than Defense Cards. In the previous playtest, some players reported that "The role of the guards seem a bit useless because the defense cards are only pointing at one specific attack card and are open to your opponents, so the player is more likely to play attack cards than defense cards". This change aims to make Defense Cards more attractive to players, as a reflection of defending is better than attacking as a company. The complete card decks can be found in Appendix A. Here, a list of cards that have interesting concepts is presented. They reflect certain concepts of information security.



(a)



(b)

Figure 4.9: Sample cards of second prototype.

4.4.2 Playtest Sessions

6 playtest sessions with 8 players were conducted with the second prototype. The players include 5 KMD Master's students, and 1 MNC company workers with a Master's degree and 1 MNC company worker with a PhD degree.



Figure 4.10: Playtest session for "Empires 2.0" on December 10th, 2017.



Figure 4.11: Playtest session for "Empires 2.0" on December 13th, 2017.



Figure 4.12: Playtest session for "Empires 2.0" on January 13th, 2018.

Feedback

Here, to gain quantitative feedback from the playtest sessions, pre-play and post-play surveys are created. The detailed content of the survey can be found in Appendix D and Appendix E. All players filled out the two surveys. The result of the surveys is discussed in the Evaluation session below.

Interviews were also conducted as a follow-up, where players were asked in detail about their game play experience, what they have learned, and suggestions. Some feedback from the interviews include: the images are proved to be helpful in players' understanding and memories of the content.

During the playtest sessions, players were observed closely. Results of the game play are quite balanced. For example, even when one goes broke, one can come back by earning money from people or Event Card.

Some suggestions are made for future improvement, such as defense Cards might be better hidden. The question is how to practically do it when one has to pay the price for them? Another interesting suggestion from a player is to have a way for underdog to come back, for example players can take a loan from the bank, add more cards without money.

4.4.3 version 2.0.0: "Aegis: The Invisible War"

As the game play has been finalized and the basic design has been proven non-problematic, I started the final design of the game using Adobe Illustrator. This

step is equally important and crucial as any other step during the project, as this determines the brand image of the product.



Figure 4.13: Complete design of Aegis: The Invisible War.

4.4.4 Evaluation

Evaluation is first made through qualitative methods with the first prototype, including interviews with players before game play, observation and record during game play, and discussion after game play.

All 9 players were asked about their education background, interests and knowledge about information security, interests and experience of board games. All the players are either Master’s students or workers with Master’s Degree. 2 of them are interested in information security and have had plenty of previous knowledge of the topic. The rest of them do not have any previous knowledge. 8 of them are interested in board game and regular board game players. Only 1 of them do not play board game regularly, and has only played limited numbers of games before.

During playtest sessions, the behaviour of players and interaction between players are observed. All players who have board game experience before get really engaged in the game play, showing proof that the game experience is fun and playful. The players experience excitement when they are leading, frustration when they go into debt, and disappointment when a card they planned to purchase got taken by their opponent first. Some got jokingly competitive when one was

being attacked fiercely. The 1 player who is unfamiliar with board game playing shows frustration when he fails to comprehend the rules.

The playfulness of the game is further confirmed during the discussion sessions after the game play. 8 out of 9 players find the game fun and entertaining to play, and they are very engaged in the game. Those who were not interested in the topic of information security before are asked if through the game, they get more interested in the topic. All of them responded positively. All players are asked if they can remember some of the content of the cards. Players remember the description of 1 Attack Cards that have strong effect, 2) Defense Cards that have unique effect, 3) the cards that put them in danger.

Evaluation for the second prototype involves a combination of quantitative data and qualitative feedback. During the pre-play survey, all players are asked their education background, interests and experience in board game, interests and previous knowledge in information security. During the post-play survey, all players are asked to rate the game over different aspects, based on a standard Game Evaluation Sheet, adjusted to suit the purpose of a board game [18]. Then they are asked about information security in relation to the game. The players are then engaged in a follow-up interview to discuss in detail their game play experience, what they have learned and suggestions.

From the pre-play survey, it reports that 4 players are female and 4 players are male. 6 of them are pursuing Master's degree, 1 is working with a Master's degree and 1 is working with a PhD degree.

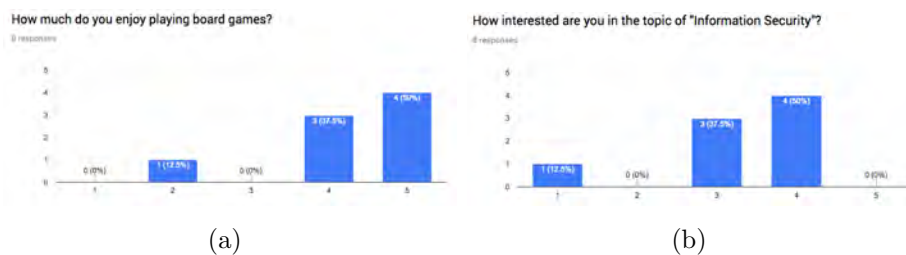


Figure 4.14: Pre-play survey result on interests of board game and information security.

Interesting, more players enjoy playing board games than learning about information security. This proves that combining board game can be a good way to intrigue people's interests in information security. This is further proved in the post-play survey, where all players think the theme fits the game mechanisms, and the rate for the game concept reaches over 8 out of 10 in average.

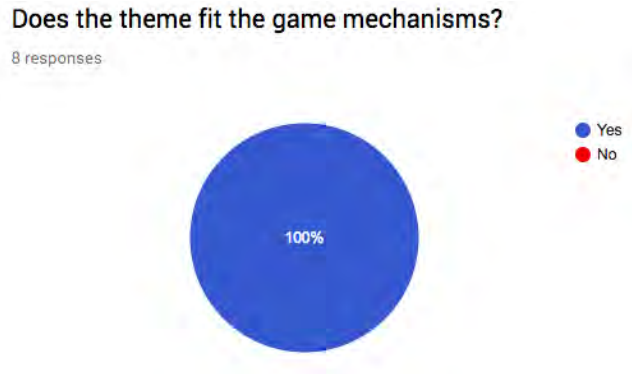


Figure 4.15: Post-play survey result on if the theme fits the game mechanisms.

The survey shows that the players only take basic actions to protect their information. 4 of them claim to think about information security in their personal life without taking any action, while 4 of them claim to take simple actions.

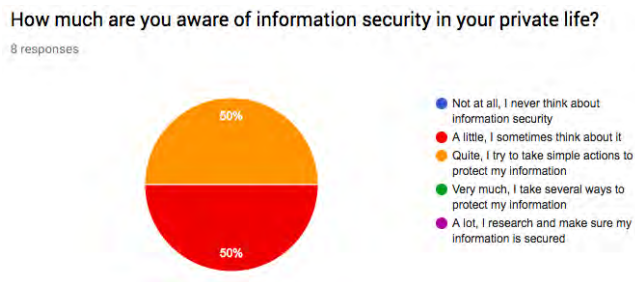


Figure 4.16: Pre-play survey result on information security awareness in private life.

It seems that the situation for working environment is slightly better.

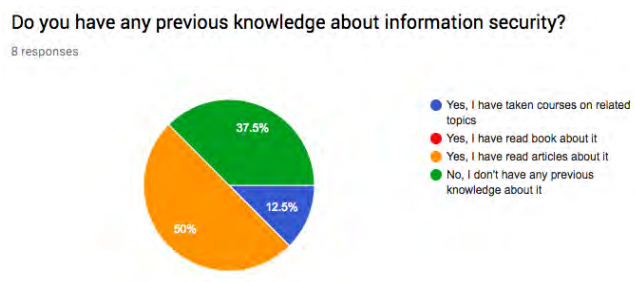


Figure 4.17: Pre-play survey result on information security awareness in working environment.

This result, in its limited scale, reflects the lack of information security awareness even in a highly educated sample group. One of the players claims to be very interested in information security, and have taken courses about the topic. However, it seems that the interests and knowledge about the topic does not directly result in a high information security awareness in real life. As for the rating of the game, the result is quite optimistic. Players rate 8 out of 10 in average on how much they enjoyed playing the game.



Figure 4.18: Pre-play survey result on how often players play board game.

Regardless of how often players have played board game before, they all enjoy the game, which proves that the game is suitable for beginners in board game to hard-core board game fans.

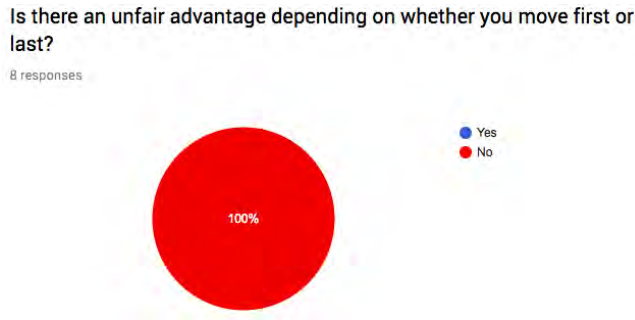


Figure 4.19: Post-play survey result on first player advantage.

The result on first player advantage proves that the second prototype has solved the problem in the first prototype, as all players claim that there is no first player advantage.

Other ratings on the games including complexity, instruction clearness, waiting

time, total game length and luck-strategy balance all result from 4-7, indicating a reasonable setup of game play in these aspect.

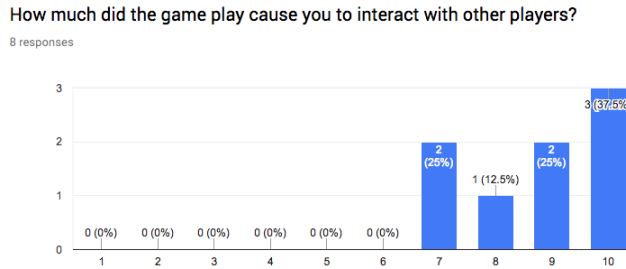


Figure 4.20: Post-play survey result on interaction.

Among them, the rating on interaction with other players scores high as 8.75 out of 10 with 3 players rating 10, proving that the game offers sufficient interaction between players.

When it comes to the after-play result on information security, except for 1 player, all 7 players claim to become more interested in the topic after playing the game.



Figure 4.21: Post-play survey result on interests.

All these 7 players rate 4 out of 5 on their current interests in the topic of information security, with 1 raising from 1 to 4, and 1 raising from 3 to 4. They also all think that the game increases their information security awareness. When asked if they have learned anything about information security, 6 claim to have learned something. Some of them learned that "there are many types of attacks and also ways to defend yourself from it", "what some hacker techniques are called, and how to defend against those attacks", "it is important to invest on information security protection against all kinds of attacks", "counter actions to

prevent attempts to steal information", and one specifically mentioned "Acting" attack card, which is a typical social engineering attack. One of the players explains that he is already quite familiar with the topic, therefore he is more focused on the strategy instead of the content. He would have learned more if he read more of the card content. Here, it appears that only 1 player did not enjoy the game as much as everyone else. This player is the one giving the lowest rate on the fun of the game (6 out of 10). This player is also the only one claiming to not become more interested in the topic, not become more aware of information security and have not learned anything. Combining the observation made during the playtest session, a possible explanation for this could be that the player was not paying attention during the game play experience. The player seems uninterested from the beginning, did not follow the game instruction, played on mobile phone most of the time when other players were making actions and did not strategize to make the best move. This result proves the hypothesis that the game is better enjoyed when players try their best to strategize.

In conclusion, the playtest sessions have successfully prove that "Aegis: The Invisible War" provides a fun and entertaining game play, and intrigue players' interests in the topic of information security, thus raising awareness in information security. Although the learning experience defers individually, most players do learn some attack and defense techniques to a certain extent from the game play, if they are concentrated during the process. However, this can still be improved in the future through changes of card design and game flow.

4.4.5 Main Takeaways

The main takeaways during this long journey of making "Aegis: The Invisible War" to its current stage can be summarized in two parts: design and content creation.

Through different versions of the project, I used different tools to make prototypes of different stages. In earlier stage, the focus should be on efficiency, as most of the design, content and concept might be changed. As the project evolves, the need for more complex and professional design tools surface. During the process, I learned how to use Adobe InDesign and Illustrator.

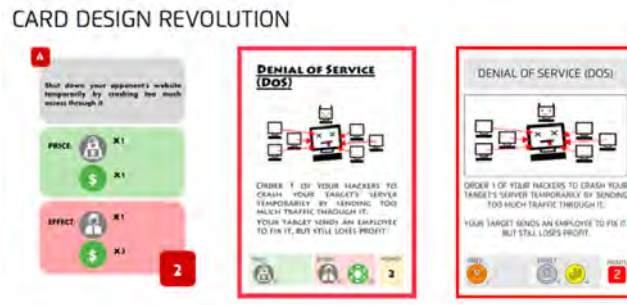


Figure 4.22: Card design evolution.

Another main takeaway lies on the process of content creation. The biggest challenge of this project is how to translate the abstract concept of information security into the design of a physical board game. It is a process of iteration and modification that involves academic research, tryouts, ideations and playtests. Here I list the concepts that were translated into game play and game content:

- The CIA tripod plus non-repudiation was used to create basic card content. From brainstorming what kind of attacks might endanger confidentiality, integrity, availability and non-repudiation of certain information, it is more systematic to create Attack Card content.
- The game elements include financial resource and human recourse. This is based on the reality that in order to protect information, one must invest either financially or invest on an expert or both. These invest sometimes will not have an immediate effect, but are crucial for the company in a long run. Furthermore, companies usually have limited recourse to invest on. This is when the manager must make decision on what is best to invest on.
- The concept of certain Attack and Defend Card requires another basic card or other cards to be effective is based on the vector concept in cyber security. There are fundamental actions or equipments that the company needs to have as a basic defense or attack in information security.
- The rule that Defense Card has to be played before its designated Attack occurs also reflects a rule in information security, as the company must equip itself with defense before attack happens. It is always too late when a certain type of attack is happening that the company realizes what kind of defense should be effective.

- In "Aegis: The Invisible War", most Attack Cards can be prevented by certain Defense Cards. However, not all Attack Cards has a Defense Card. This is a reflection that not all information attacks can be prevented. Sometimes, a breach is unavoidable. However, having basic and strong information security can lower the possibility of that happening.
- The concept of Event Cards reflects that sometimes information security can be compromised outside of a vicious human action. Random event such as natural disaster can also cause damage on information security. Companies should also take them into consideration when building a proper information security system.
- The fact that Defense Cards give more points than Attack Cards reflects a morality balance. As a company, the priority should be building up its information security defense. Attacking other companies' information can result in severe consequence.
- Certain Defense Cards such as Chief Information Security Officer or Information Security Awareness Training do not protect players from certain Attack Cards. However, they increase the efficiency of defense and lower the possibility of being attacked. This is a reflection of basic information security setup in the company to increase the overall information protection. They are the foundation to a strong information security environment and they are an absolute must for any company involved with digitalization.

Chapter 5

Conclusion

5.1 Concept Validation

This project aims to create a board game that intrigues people's interests in the topic of information security. The process to reach that goal has been a long and weary journey. It has reached a milestone with the completion of this document.

The academic research set out a firm foundation where the whole project is built on. It establishes the problem that the project sets out to solve: despite the importance of information security awareness, lack of interests from the audience has been a big challenge to information security awareness training. As there has no game previously made for that purpose, the contribution and significance of the project is validated.

The final design of the game is completed with consideration of as many aspects as the designer can reach within the scope of this project. It offers a clear definition of the game, market positioning, as well as paper materials for the game, such as Rule Book, user boards, and card decks.

The document keeps a record of iterations of the game development. Through different stages of the project, the concept, including the naming, game flow, and art style, has gone through significant changes. Those changes are validated through ideation sessions and play test sessions, where feedback from the players are analyzed and taken into improvements. This journal not only shows the growth of the game, but also the learning process of the designer. Through each stage, the designer requires new skills, learns new tools and improves certain abilities. The process also reflects possible contribution of this project on how to translate abstract concept into game design.

Combined playtest sessions have proven that the design at the current stage has achieved the original goal of this project: "Aegis: The Invisible War", a multi-player card-based board game ready for the general board game market that provides a fun and playful experience with its diverse resource, dynamic

game play and multi-level expandable card decks, through which players get more interested in the theme - information security, and potentially learn about basic attack and defend techniques.

5.2 Possible Improvements

While the end of this thesis marks the end of the project, there are so many elements that still need to be improved regarding the game itself.

- 1) Completion of card design, which requires a professional graphic designer.
- 2) Extension of card content, which requires a or a team of computer science expert and information security experts.
- 3) Improvement of game flow and rules, which can be more efficient to collaborate with a professional game designer.
- 4) More playtest with people from different background.
- 5) Quantitative survey and quizzes during playtest.

Through those, I aim to produce a prototype with a basic card deck and other elements that can be commercially used and played for a full board game experience.

5.3 Extension of Concept

Although the plan for the game with my own power ends with a playable prototype ready for commercial use, the board game itself can be further brought to the market with fundraising website and recruitment of a team working on it. Once it has been proven successful on the board game market, it can also be brought to computer-based platforms, which offers more engaging visuals and game play experience.

References

- [1] Aitel, D. Why you shouldn't train employees for security awareness. July 18, 2017. Accessed at November 21, 2017. <https://www.csoonline.com/article/2131941/security-awareness/why-you-shouldn-t-train-employees-for-security-awareness.html>.
- [2] Alberts, C., and Dorofee, A. *Managing information security risks: The OCTAVE (SM) approach*. Addison Wesley, 2002.
- [3] Chia, T. Confidentiality, integrity, availability: The three components of the cia triad. August 20, 2012. Accessed at January 29, 2018. <http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/>.
- [4] Crookall, D., and Arai, K., Eds. *In Simulation and gaming across disciplines and cultures: ISAGA at a watershed*. SAGE, Thousand Oaks, CA, 1995.
- [5] Daniel, S. How i socially engineer myself into high security facilities. October 21, 2017. Accessed at November 21, 2017. https://motherboard.vice.com/en_us/article/qv34zb/how-i-socially-engineer-myself-into-high-security-facilities.
- [6] Dhillon, G., and Backhouse, J. Technical opinion: Information system security management in the new millennium. *Commun. ACM* 43, 7 (July 2000), 125–128.
- [7] Erickson, J. *Hacking: the art of exploitation*. No Starch Press, 2008.
- [8] Garris, R., Ahlers, R., and Driskell, J. E. Games, motivation, and learning: A research and practice model. *Simulation & Gaming* 33, 4 (2002), 441–467.
- [9] Gellineau, O. Elements of a security awareness training program. April 24, 2015. Accessed at November 21, 2017. <https://www.csoonline.com/article/2131941/security-awareness/why-you-shouldn-t-train-employees-for-security-awareness.html>.

REFERENCES

- //www.linkedin.com/pulse/elements – security – awareness – training – program – obika – gellineau/.*
- [10] Information Security Forum. The standard of good practice for information security 2016. Tech. rep., Information Security Forum, 2016.
- [11] Moore, M. E., and Novak, J. *Game Development Essentials: Game Industry Career Guide*, 1st ed. Delmar Learning, 2009.
- [12] Ponemon Institute. 2017 cost of data breach study: Global overview. Tech. rep., IBM Security, 2017.
- [13] Risk Based Security. The 2016 data breach quickview report. Tech. rep., Risk Based Security, 2017.
- [14] Ryan, J. E. *A Comparison of Information Security Trends Between Formal and Informal Environments*. PhD thesis, Auburn, AL, USA, 2006. AAI3225287.
- [15] Schell, J. *The Art of Game Design: A Book of Lenses*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008.
- [16] Symantec. The internet security threat report. Tech. rep., Symantec, 2017.
- [17] Thomson, K.-L., and Von Solms, R. Information security obedience: A definition. *Comput. Secur.* 24, 1 (Feb. 2005), 69–75.
- [18] Whitehill, B. Game evaluation sheet. Accessed at January 29. 2018. *http : //thebiggamehunter.com/game – evaluation – sheet/.*

Appendix

A Card Lists

A.1 Attack Cards

Table A.1: List of Attack Cards.

Name	Description	Price	Effect	Points
Denial of Service	Order 1 of your hackers to crash your targets server temporarily by sending too much traffic through it. Your target sends an employee to fix it, but still loses profit.	1 Hacker to work	2 Coins, 1 Employee to work	1
Corporate Espionage	Send 1 of your hackers to go undercover in your targets company. Your spy will need some money. Your target hires your spy as an employee, while losing profit to you because the information the spy has been leaking to you.	Lose 1 Hacker permanently, 1 Employee to work, 2 Coins	Gain 1 Employee, Pay 4 Coins each round	5

Continued on next page

Table A.1 – continued from previous page

Name	Description	Price	Effect	Points
Sticky Fingers	Send 1 of your hackers to research about 1 of your targets employee. After getting to know the targets interests, approach the target at a bar after work. Steal the targets ID card.	1 Hacker to work, 2 Coins	1 Coin	1
Ninja	Once you have an ID card and password, you send 1 of your hackers to sneak into your targets building at night and steal information on the targets computer.	1 Hacker to work	Pay 3 Coins	5
Route Hijacking	Send 1 of your hackers to hack into your targets wifi router. Youll get access to the information being transmit through it.	1 Hacker to work	Pay 2 Coins	1
MITM	Once you have access to your targets internet connection, you order your hacker to alter the information.	1 Hacker to work	5 Coins	3
Password	Send 1 of your hackers to research about 1 of your targets employee. Getting to know the targets interests makes it easier to process the targets passwords of company accounts.	1 Hacker to work	1 Coins	1

Continued on next page

Table A.1 – continued from previous page

Name	Description	Price	Effect	Points
Cloud Access	Once you have access to your targets internet connection, you order 2 hackers to hack into your targets server. You now have access to all your targets information.	2 Hacker to work	Pay 5 Coins	6
Takeover	You used the vulnerability scanner and exposed weakness in your targets manufacturing floor control center. Order 1 hacker and 1 employee to takeover the control system and shut down the operation.	1 Hacker and 1 Employee to work	4 Coins, 1 Employee & 1 Guard to work	4
Vulnerability Scanner	Order 1 of your employees to purchase a vulnerability scanning software. Use it to expose vulnerabilities in your targets security system.	1 Employee to work, 1 Coins	1 Coin	2
Blackout	Send 2 of your employees to cut off your targets electricity cables and shut down the buildings electricity supply.	2 Employee to work, 1 Coins	1 Employee, 3 Coins	2
No Connection	Send 2 of your employees to cut off your targets internet cable and shut down the buildings internet supply.	2 Employee to work, 1 Coins	1 Employee, 3 Coins	2
Continued on next page				

Table A.1 – continued from previous page

Name	Description	Price	Effect	Points
I'm watching you	Hack into your opponants security camera system. This will increase your possibility of succeeding in any physical invasion.	1 Hacker to work	" +1 on your dice results of physical invasion attack. +1 on dice requirements of defence against physical invasion attack."	1
Rerouting	You order 1 of your guards to change the router setting and disturb your targets internet connection.	1 Hacker to work	1 Guard, 3 Coins	3
Ransomware	Once you have infected your targets computer, or have found a weakness in the system, you conduct a ransomware attack, encrypt targets files, and ask for ransom.	2 Hackers and 1 Employee to work	1 Employee and 1 Guard to work, Pay 5 Coins	7
Rumor	Send 1 of your employees to investigate your targets history and spread news that halm your targets reputation online.	1 Employee to work	2 Coins	1

Continued on next page

Table A.1 – continued from previous page

Name	Description	Price	Effect	Points
Time Bomb	Once you have access to your targets files, order 1 employee and 1 hacker to alter information. This will lead to false analysis and harm your targets profit. Throw the dice to decide how many coins your target loses.	1 Hacker 1 Employee to work	Dice Result	5
Cloud Storage	Order 1 employee to research on the cloud storage service your target uses. Then 2 of your hackers hack into the cloud storage account.	2 Hackers and 1 Employee to work	Pay 5 Coins	4
Hacking 4.0	Order 1 hacker to hack into your targets IoT (Internet of Things) system through an unsecured IoT device.	1 Hacker	1 Coin	1
Acting	Contact your opponent's manager as a floor designer, ask for a office tour, enter the building and witness company secrets.	1 Hacker to work	Pay 3 Coins	4
Phishing	Send an email that contains a virus to all employees of your target. If succeed, you will get access to the information on that computer. If fail, no point gained, discard the card. Thorw dice twice to determine the result.	1 Hacker to work	Pay 1 Coins	3

A.2 Defense Cards

Table A.2: List of Defense Cards

Name	Description	Price	Effect	Points
Background Check	Assign 1 of your employees to run regular thorough background check of potential employees, making sure the company only hires people with the right intuitive.	1 Employee to work each round	Deactive "Spy"	6
Security Guard	Send 1 of your guard to check your employees identity during working hours.	1 Guard to work each round, 1 Coins	Deactive "Sticky Fingers"	3
Security Gate	Send an employee to set up a security check-point with a scanner at the entrance of your company building.	1 Guard, 3 Coins	Deactive "Sticky Fingers"	3
Biometric Scanner	Set up a biometric security system that requires fingerprint identification when your employees enter the building.	1 Employee, 3 Coins	Deactive "Sticky Fingers"	3
Encryption	Order 1 of your guards to establish a data encryption system: all information sent between users and server is encrypted and can only be open with private key. Your guard will need 1 Employee to work with him.	1 Guard and 1 Employee	Deactive "MITM" "Cloud Access"	6
Continued on next page				

Table A.2 – continued from previous page

Name	Description	Price	Effect	Points
Arm Up	Order 1 of your guards to purchase a better router, invest in security software that detects suspected hijacking, and establish a stronger router system.	1 Guard to work each round, 4 Coins	Deactive "Route Hijacking"	8
Chameleon	Order 1 of your guards to set up a password security system that requires your employees to change their passwords every month.	1 Guard,	Deactive "Pass"	3
Cloud Nine	Order 1 of your employees to research a secure server provider. Order 1 of your guard to set up a more advanced server that is stronger, guarded and encrypted.	1 Guard, 1 Employee, 5 Coins	Deactive "DOS" "Access to the Cloud"	9
Bayesian Filtering	Order 1 of your guards to install an advanced filtering software that detects vicious emails for all incoming emails	1 Guard, 2 Coins	+1 on the dice result for Phishing	3
Classroom	Order 2 of your guards to hold information security training for your employees. This will increase the difficulty of attacks involving your employees.	2 Guards	Password, Sticky Fingers uneffective. +1 on dice requirements of Phishing, Party Night."	2/Employee

Continued on next page

Table A.2 – continued from previous page

Name	Description	Price	Effect	Points
Justice	Order 1 of your guards to trace back IP addresses of any cyber attacks. If succeed, you can report to the authority.	1 Guard each round	If succeed, permanently lose a Hacker	5
Chief Information Security Officer	Hire a chief information security officer. the CISO will set up information security policy for the company and increase information security awareness in general.	3 Coins each round	+1 all dice results	8
Know Your Weakness	Order 1 of your guard to purchase a vulnerability scanning software. Use it to expose vulnerabilities in your security system and enhance the weakness.	1 Guard, 1 Employee to work each round, 3 Coins	Deactive "Vulnerability Scanner"	5
Firewall	Order 1 guard to set up an advanced firewall: a guarding computer in between all connections.	1 Guard, 3 Coins	Deactive "Implant", "To the Cloud"	7
Update Armer	Order 1 employee to update all hardware devices system regularly.	1 Employee to work each round	Deactive "I see you", "Hacking 4.0"	6
All roads to Rome	Order 1 guard to set up a parallel network system for less protected devices such as IoT devices and cameras.	1 Guard	Deactive "I see you", "Hacking 4.0"	4

Continued on next page

Table A.2 – continued from previous page

Name	Description	Price	Effect	Points
Bodyguard	Hire a security company to protect your MVPs (Most Valuable Player). They are the ones who know important company information.	2 Coins each round	+1 all dice results related to physical harm of your employees	5
Trust-but-verify	Order 1 guard and 1 employee to Establish verification process among employees for actions that will endanger vital information.	1 Guard, 1 Employee	Acting, Time Bomb, MITM ineffective. +1 on dice requirements of Party Night.	8
Partner	Order 1 employee to research on a secure and safe cloud storage service. Invest on better cloud security.	1 Employee to work, 2 Bits	Deactive "Go Around"	6
PR	Establish a PR department to motinor and deal with negative news fast and efficient before any damage happens.	2 Employee to work each round	Deactive "Rumor"	6
Blockchain	Introduce blockchain technology to ensure data integrity. This will prevent any unauthorized modification of your information.	2 Guard each round	Deactive "Implant"	8

Continued on next page

Table A.2 – continued from previous page

Name	Description	Price	Effect	Points
Partner	Order 1 employee to research on a secure and safe cloud storage service. Invest on better cloud security.	1 Employee to work, 2 Bits	Deactive "Go Around"	6
UPS	Invest on a backup electricity power supply.	3 Coins	Deactive "Black-out"	4
Stay Connected	Invest on a backup internet connection.	3 Coins	Deactive "Connection Failed"	4
Backup	Order 1 employee to establish backup process on all information-holding devices.	1 Employee, 3 Coins	Deactive "Flood" "Ransomware"	4
Security Room	Set up a security room monitoring all the cameras in your building. Send 1 of your employees on duty. This will give you the possibility to catch any physical invasion attack. Throw the dice to determine the result.	1 Employee to work each round, 5 Coins	If succeeds, the attackers worker stays in the working area for another round	8
Virus Scan	Invest on a strong virus scan software.	3 Coins	"Phishing" "Ransomware"	4

A.3 Event Cards

Table A.3: List of Event Cards

Name	Description	Succeed	Fail	Dice
Pizza Night	Send 1 of your employees to disguise as a pizza delivery guy, send overdue pizzas to your targets office.	3 Employees rest	Lose 1 Employee permanently and pay 5 Coins fine	3,4
Blackmail	Kidnap an employee and blackmail your opponant with vital company secrets	Pay 5 Coins and loses 1 Employee permanently	Lose 7 Coins and 2 Employee permanently	4,5
Fire	Set your opponant's building on fire at night	loses 14 Bits and 2 Employees to work	You lose 5 Coins and 1 Employee permanently	2,3
Party Night	Disguise as a stripper to your opponant's office during their party	Pay 3 Coins	1 Employee to work and 2 Coins	3,4
Secret Path	Dig a tunnel to your opponant's basement and steal their server physically	Pay 4 Coins	2 Employees work for 2 Rounds, 2 Coins	4,5
Flood	A flood destroy your data center	5 Coins	5 Coins	4,5
Squirrels	Squirrels eating cables	1 Employee to work, 3 Coins	1 Employee to work, 3 Coins	3,4
Continued on next page				

Table A.3 – continued from previous page

Name	Description	Succeed	Fail	Dice
Bribe	Offer money to a employee of your opponant and get vital company secrets	1 Employees to work, 2 Coins	1 Employee to work, 5 Coins	2,3

B Card Decks

B.1 Attack Cards

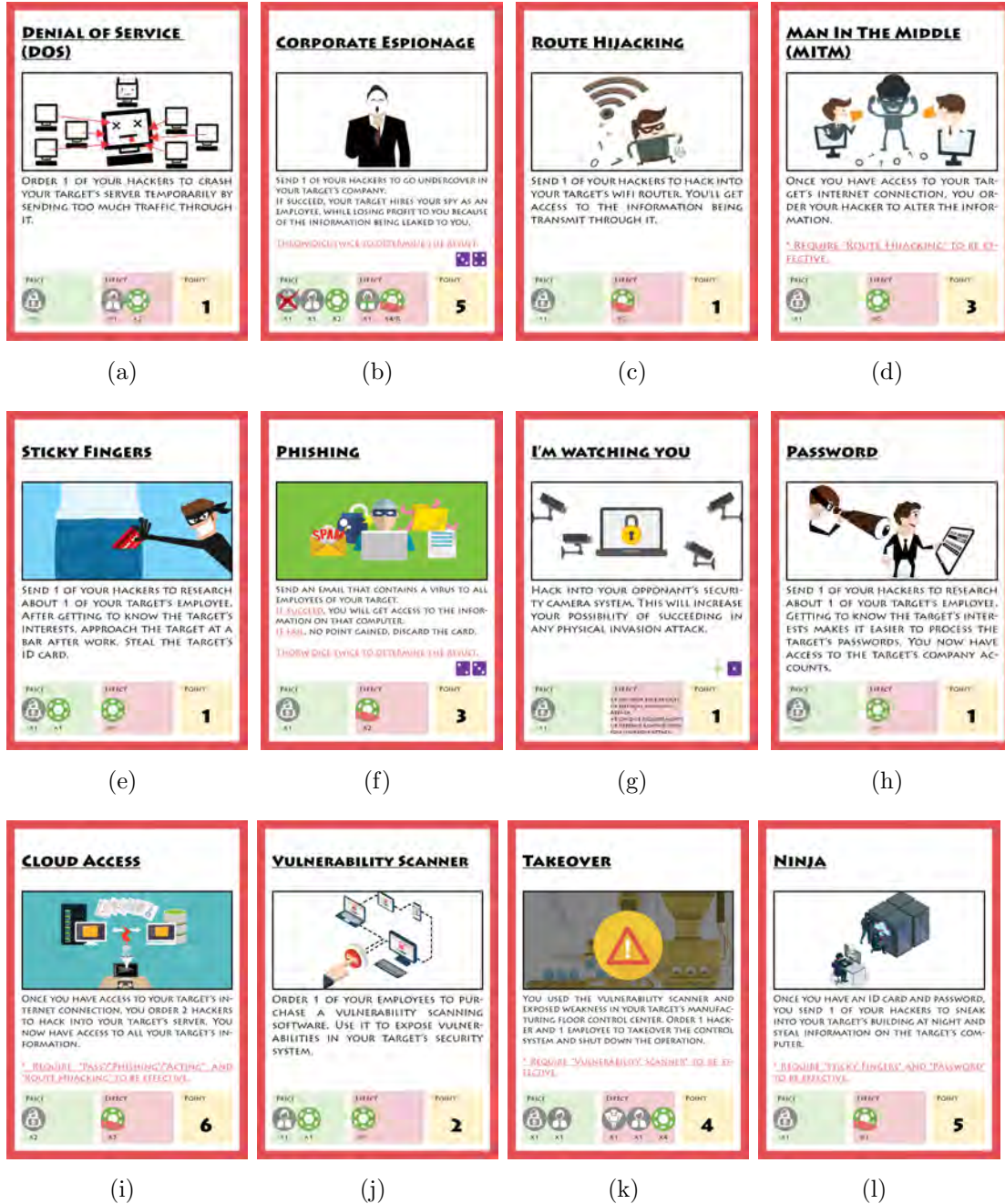


Figure B.1: Design of all Attack Cards.



Figure B.2: Design of all Attack Cards.

B.2 Defense Cards



Figure B.3: Design of all Defense Cards.

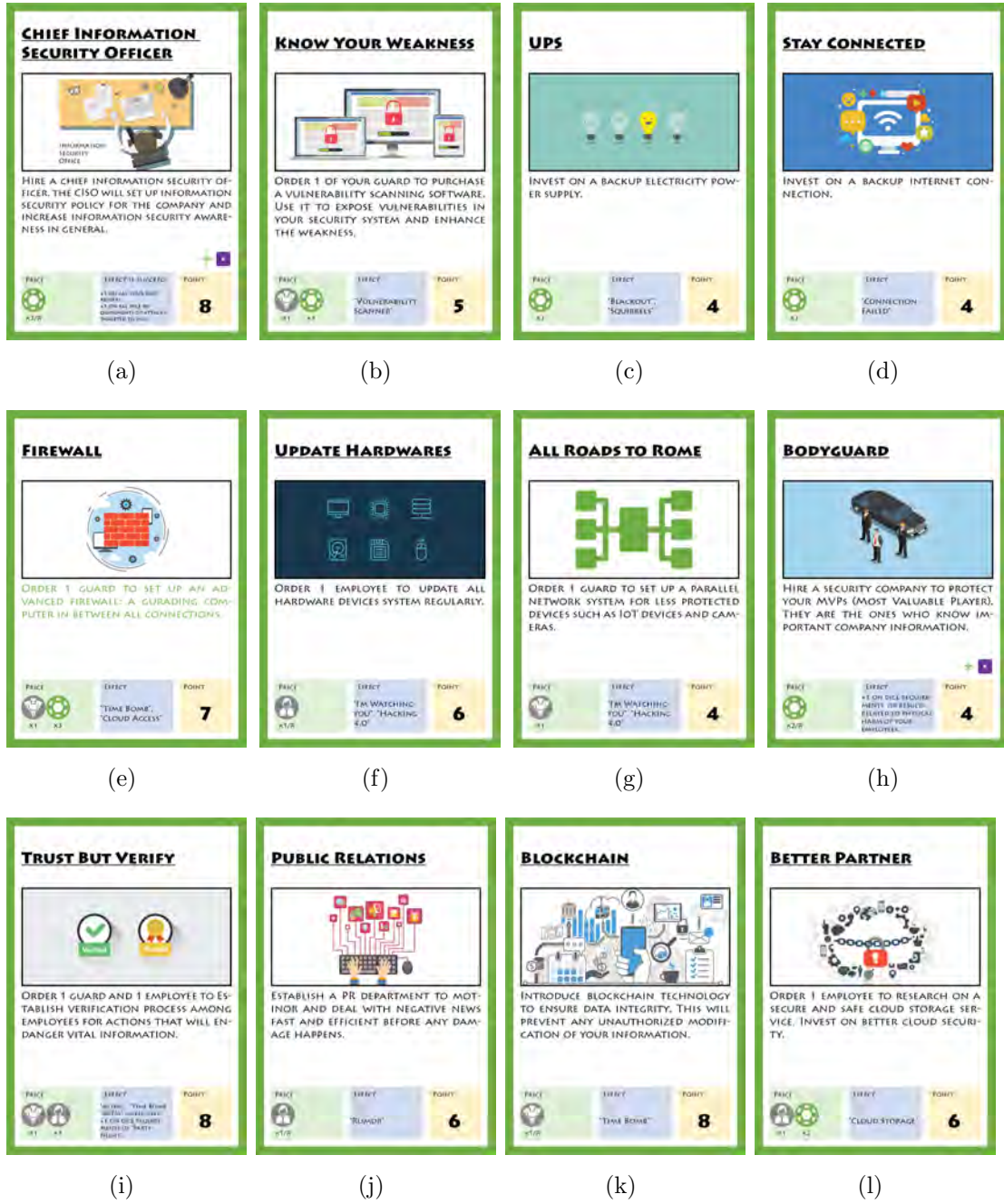
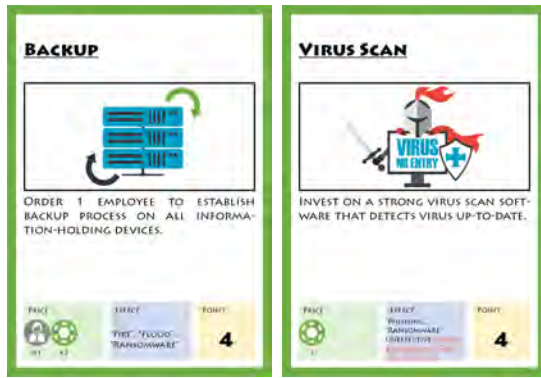


Figure B.4: Design of all Defense Cards.



(a)

(b)

Figure B.5: Design of all Defense Cards.

B.3 Event Cards

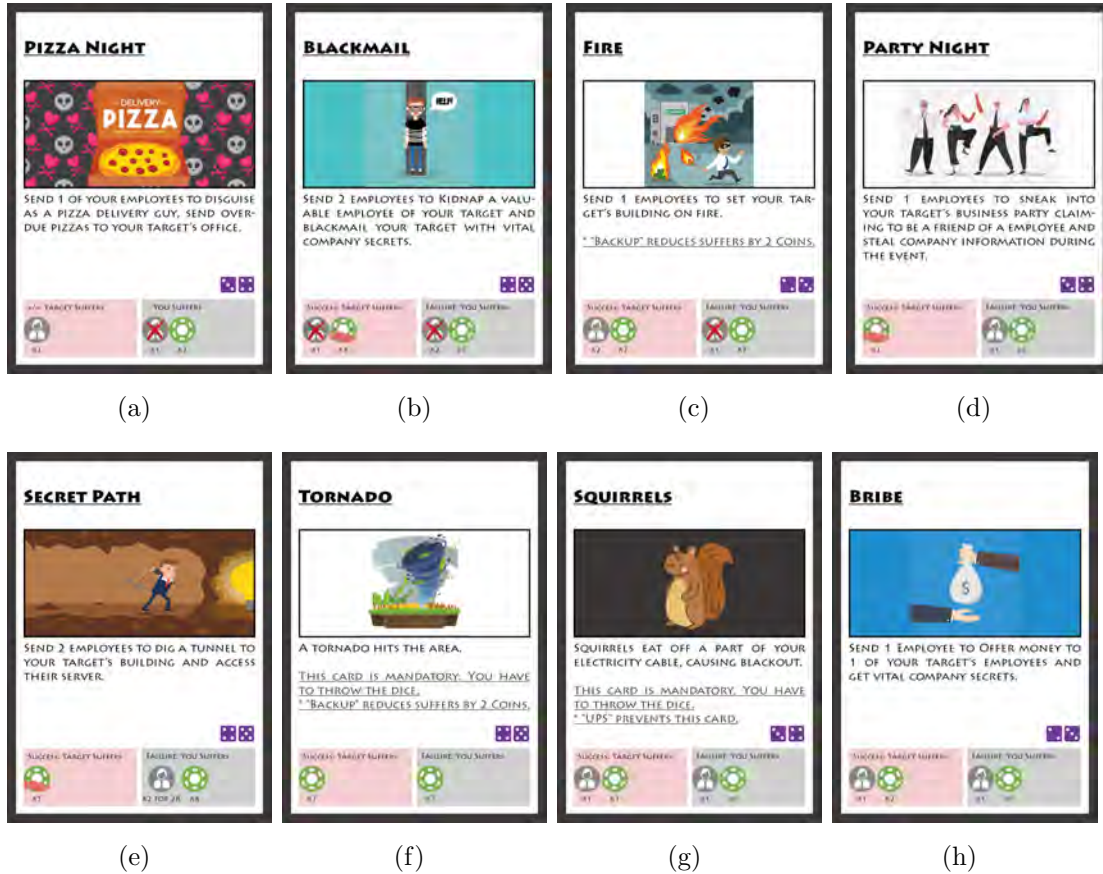


Figure B.6: Design of all Event Cards.

C Reference of Card Content

C.1 Attack Cards

- Erickson, J. *Hacking: the art of exploitation*. No Starch Press, 2008.
- Mitnick, Kevin D., and William L. S. *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2011.

C.2 Defense Cards

- Information Security Forum. The standard of good practice for information security 2016. Tech. rep., Information Security Forum, 2016.

D Pre-play Survey

Aegis Project: Survey before Playtest

Thank you for participating in the Aegis project.

* Required

Skip to question 1.

About You

1. Name *

2. Gender *

Mark only one oval.

Male

Female

Prefer not to say

Other: _____

3. Highest Education *

Skip to question 4.

About Gaming

4. How often do you play board game? *

Mark only one oval.

1 2 3 4 5

Never Very often

5. How much do you enjoy playing board games? *

Mark only one oval.

1 2 3 4 5

Not at all Very much

6. Have you played the following board games?

Check all that apply.

Netrunner

Magic: The Gathering

Above and Below

Risk

Dungeons & Dragons

Skip to question 7.

Figure D.1: Pre-play survey.

About Information Security

7. How interested are you in the topic of "Information Security"? *

Mark only one oval.

1 2 3 4 5

Not at all Very much

8. Do you have any previous knowledge about information security? *

Mark only one oval.

- Yes, I have taken courses on related topics
- Yes, I have read book about it
- Yes, I have read articles about it
- No, I don't have any previous knowledge about it

9. How much are you aware of information security in your private life? *

Mark only one oval.

- Not at all, I never think about information security
- A little, I sometimes think about it
- Quite, I try to take simple actions to protect my information
- Very much, I take several ways to protect my information
- A lot, I research and make sure my information is secured

10. How much are you aware of information security in your working environment? *

Mark only one oval.

- Not at all, I never think about information security
- A little, I sometimes think about it
- Quite, I try to take simple actions to protect my information
- Very much, I take several ways to protect my information
- A lot, I research and make sure my information is secured


Powered by
 Google Forms

Figure D.2: Pre-play survey.

E Post-play Survey

Aegis Project: Survey after Playtest

* Required

About Aegis: The Invisible War

1. How much did you enjoy playing this game? *

Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Not at all	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	I loved it!

2. How do you like the concept of this game? *

Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Not at all	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Terrific!

3. Does the theme fit the game mechanisms? *

Mark only one oval.

- Yes
 No

4. Is there an unfair advantage depending on whether you move first or last? *

Mark only one oval.

- Yes
 No

5. How complex is the game? *

Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Very simple	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Very complicated

6. Is the game instruction easy to understand? *

Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Very simple	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Hard to understand

7. Luck vs. Strategy to win the game? *

Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Pure luck	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Only strategy

Figure E.1: Post-play survey.

8 Was the game too short, too long or just right? *
Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Too short Too long

9 How much did the game play cause you to interact with other players? *
Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Never All the time

10 How much waiting between your turns? *
Mark only one oval.

1 2 3 4 5 6 7 8 9 10

Very little Too much

About Information Security

11 Are you more interested in the topic of "Information Security" after the gameplay? *
Mark only one oval.

Yes
 No

12 How interested are you in the topic of "Information Security" now? *
Mark only one oval.

1 2 3 4 5

Not at all Very much

13 Do you think the gameplay increase your information security awareness? *
Mark only one oval.

Yes
 No
 Other _____

14 Have you learned anything about information security during the game play? *
Mark only one oval.

Yes
 No
 Other _____

15 If yes, what have you learned?


Powered by
 Google Forms

Figure E.2: Post-play survey.