Understanding the dynamics of Information Security Investments. A Simulation-Based Approach

By

Anaely Aguiar Rodríguez

Thesis submitted in partial fulfillment of the requirements of
Master of Philosophy in System Dynamics
(Universitetet i Bergen), Master of Science in System
Dynamics (New University of Lisbon)
and
Master of Science in Business Administration
(Radboud Universiteit Nijmegen)

Supervised by
Dr. Birgit Kopainsky

System Dynamics Group
Department of Geography
University of Bergen

June, 2017

Acknowledgements

It is a great pleasure to acknowledge my deepest gratitude to Dr. Birgit Kopainsky for her valuable and keen guidance throughout this research project. Thank you for consistently allowing this thesis to be my own work, but steering me in the right direction whenever you thought I needed it.

I would also like to extend my sincere appreciation to all of the EMSD professors and staff who have made this master programme a great academic and life experience.

My special thanks to my EMSD friends: Cristian, Lize, Shruti, Ginevra and I-Chung for their true friendship and support demonstrated in these two amazing years.

I also would like to express my sincere gratitude to my mom for her enduring love and for always being by my side, even in the distance. Last but not least, thank you my David (mi tutu), your constant encouragement, advice and love, is what made this research such a rewarding journey.

Anaely Aguiar Rodríguez

June 23rd, 2017

Abstract

Today, information security breaches are steadily increasing, constantly puzzling security managers on how to make the best investment decisions to fight against cyberattacks. The problem is that there is a lack of understanding about the dynamic interaction between attackers and defender when making security investment decisions. The goal of this thesis is to develop a system dynamics model that describes the dynamic interaction between a defender, who initially invests a portion of the security budget and defers the remaining investments until security breaches occurs, known as wait and see strategy; and an attacker, who repeatedly targets and exploits the weakest link of the defense, known as weakest link strategy. The research employed qualitative and quantitative system dynamic modeling tools based on theoretical frameworks from the information security investment literature. A simulation model was built to understand the behavior of both adversaries when applying the aforementioned strategies under uncertainty and propose policy options to solve the problematic behavior. Scenario and policy analyses were conducted to test the hypothesis that under uncertainty the wait and see and the weakest link approaches, are not effective security investment strategies. Scenarios show that when uncertainty increases, it is rational for the defender to under-invest in information security and rather cope with attacks. In situations of high uncertainty, effective security investment requires acquiring knowledge about attacks and shifting from reactive to proactive investment strategies. Two policy options were proposed to improve defenders' financial performance over time, 1) information sharing among defenders and 2) higher dismissal time of attacks. By implementing information sharing policy, defenders experience a worst-before-better behavior, meaning that defenders need to be patient to perceive the benefits of this policy. Furthermore, implementing higher dismissal time of attacks entails more immediate benefits, though with managerial implications such as the need of a higher security budget. Finally, implementation of the combination of information sharing and higher dismissal time depends on the size of the firm's and the available budget (capabilities) to invest in information security.

Table of Contents

List of Figures

List of Acronyms

ALE: Annual Loss Expectation

CLD: Causal Loop Diagram

IRR: Internal Rate of Return

LHS: Latin Hypercube Sampling

NPV: Net Present Value

ROI: Return of Investment

ROSI: Return of Security Investment

SD: System Dynamics

SFD: Stock and Flow Diagram

WAS: Wait And See

WL: Weakest Link

Chapter 1: Introduction

1.1 Background Information

The internet revolution has dramatically transformed the way people, firms, and governments communicate and conduct business. However, this extensive interconnectivity has increased the vulnerability of computer systems to information security breaches (Gordon et al., 2003). Protection of their IT systems, data, intellectual property, and business processes against attacks, misuse or technical failures has become and is predicted to remain a key challenge for organizations (Anderson, 2001; Gartner, 2011, 2012; Suby & Dickson, 2015; Whitman, 2003).

IT threats can lead, for example, to the disruption of production and service processes (e.g., attack on MasterCard and Visa (The Guardian, 2010) and data theft (e.g., attack on Sony Pictures Entertainment (The Washington Post, 2014) and the disruption of more than a billion accounts at Yahoo (The Guardian, 2016)), which in turn result in economic damage, including losses in productivity and revenue, strategic disadvantages and loss of reputation (Bandyopadhyay et al., 2009). A more recent example of a world-spread cyberattack is the Wannacry ransomware attack in May 2017, which exploited Microsoft's Operating System default vulnerabilities and affected several types of companies, public institutions, universities and personal computers all over the world; demanding ransom payments via Bitcoins cryptocurrency to unblock the access to their data (The Guardian, 2017; The Telegraph, 2017). Some countries have not been affected by the Wannacry attack, yet, this does not give any indication whether these countries will not be attacked in the future (Avast, 2017). Many security incidents are attributable to cybercrime, which can be considered a growing industry (McAfee, 2014).

Information security is more than just a defensive mechanism by organizations. Information security is also a strategic variable that can help organizations gain a competitive advantage in the market (Huang et al., 2008). The importance of information security has led many organization to pay much attention to information security investment decisions and, particularly to deriving the appropriate level of these investments (e.g., Bodin et al., 2005; Cavusoglu et al., 2004, 2005; Gordon & Loeb, 2002; Huang et al., 2008). However, even with all the emphasis on security, the amount of unauthorized intrusions and security breaches are steadily increasing as it can be observed in Figure 1.

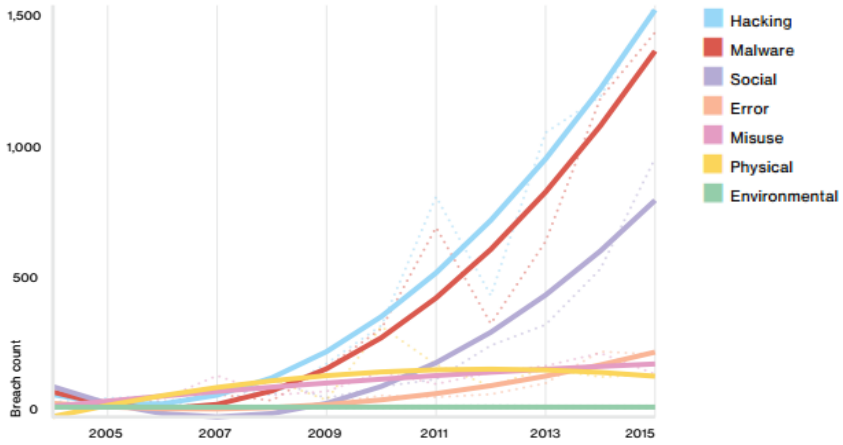


Figure 1 Number of Breaches per Threat Action Category over time (Verizon, 2016)

Organizations have responded to emerging IT security threats with high investments in IT security. As stated in Gartner (2016), the worldwide spending on IT security reached $81.6 billion in 2016, an increase of 7.9 percent over 2015, and is expected to grow further around 8 percent in following years. These figures indicate that the IT security landscape is occupied not only by technological challenges but also by financial ones, that companies face while implementing measures to prevent losses and respond to damage recovery efforts resulting from cybercrimes (Gordon & Richardson, 2004). In this context, it is of crucial importance to know how companies can effectively defend themselves against cyber-attacks.

Today, information security breaches are still common and rising as illustrated in Figure 1, constantly puzzling security managers regarding investment decisions to fight against attacks (Arora et al., 2004). Determining the right amount to spend on information security activities is linked to efficiently allocating such resources to specific security strategies. Each security strategy involves different cost, effectiveness and potential benefits; many of these are difficult to quantify (Nazareth & Choi, 2015). This struggle rises because of the uncertainty surrounding threat manifestation, damage suffered, recovery efforts and loss of reputation (Bandyopadhyay et al., 2009; Sun, 2013). Nonetheless, managers need to select security strategies in a periodic basis. Then, key economic questions for organizations arise from these facts: which of their assets (processes, systems, etc.) need which level of protection, which security countermeasures (e.g., firewalls, intrusion detection systems, security training, or security policies) lead to this protection and how much should be spent on which countermeasure? (Anderson & Schneier, 2005; Gordon & Loeb, 2002, 2006).

In the efforts to secure data and systems, research conducted by practitioners and scholars has primarily been focused on the technical aspects of information security, that is, on the questions of which assets need which level of protection and which security countermeasures lead to this protection. Research related to the economics of information security, that is, to the question of how much should be spent on security countermeasures, is still nascent (Gordon & Loeb, 2006; Huang et al., 2008). This is reasonable, because information security investments usually do not generate direct monetary benefits such as higher revenues or lower costs; their main contribution is to prevent potential economic losses from happening (Böhme & Nowey, 2008). However, given the high cost of information security measures and budget constraints, a ‘‘fully secure organization’’ is a challenging, if not impossible goal (Bodin et al., 2005; Huang et al., 2007).

1.2 Problem Formulation

One explanation for the struggle managers face when making cyber security investments could be that most managers do not fully understand the economics of investing in security as pointed out by Anderson (2001) and Gordon and Richardson (2004). Even though the vast majority of security managers are willing to use economic and financial concepts in making security investment decisions (Gordon et al., 2003), many information security issues relate to qualitative and nonfinancial concerns (Bohme & Moore, 2009) such as behavioral aspects. There are only few systemic approaches capturing the complexity of behavioral aspects in information security mentioned by Martinez-Moyano et al., (2011). As Martinez-Moyano et al., indicate, “behavioral considerations of the problem are at least as important in contributing to solutions to information security” (2011, p. 398). Such behavioral aspects may include attacker-defender interactions influencing investment decision-making in information security.

Hence, “traditional economic approaches are severely constrained by their assumptions of relationships being sequential (as in the case of game theory), deterministic (as in financial analysis), or static (as in economic analysis), and often overly simplified (small number of variables)” (Behara et al., 2007, p.1573). Traditional economic approaches do not seem to be sufficiently comprehensive for understanding attacker-defender interactions and for drawing conclusions regarding effective security investment.

Since managers struggle to make appropriate investment strategies, a model that captures the complexities of security investment decisions while allowing to explore alternative strategies, would be an invaluable aid to them.

The interactions between attackers and defenders need to consider elements such as the underlying structure that generates long-term investment behavior, nonlinearities, feedback mechanisms, delays, learning, etc.; which are vital for improving understanding on adversarial decision processes and behavior (Martinez-Moyano et al., 2015). These factors form the basic building blocks for the methodology of System Dynamics that uses computer simulation modeling for policy analysis and design in complex dynamic systems (Sterman, 2000).

This thesis develops a System Dynamics model that integrates existing theoretical frameworks on information security investments. The model describes the dynamic interactions between:

- A defender, who faces uncertainty about the attackers' attack strategies, initially investing a portion of the budget and defer the remaining investments until security breaches occur (see Wait-and-see-approach in Gordon et al., (2003))[1], and
- An attacker who repeatedly targets the weakest link and exploits this advantage, as demonstrated in the economic model developed by Bohme & Moore (2009)[2].

This leads to defenders adapting their strategies over time based on the reported successful attacks. By using computer simulation, the iterative process of attack and defense in three security vectors[3] (A, B and C) is captured, exploring the balance between proactive and reactive security investment and later analyzing the model through scenario and policy options simulations under uncertainty. Thus, this study presents a hypothesis stating that with the representation of Wait-and-see and Weakest Link Approaches in an integrated dynamic framework, there might be unintended consequences for attackers and defenders over time. When making investment decisions under different uncertainty levels, WAS and WL will not be effective approaches anymore. In this context, the need of a dynamic framework to test this hypothesis, is what motivates this thesis.

[1] The defender behavior is characterized by the Wait-And-See approach, which can be explained by Gordon et al. (2003) as "before investing in information security, it may be advisable to wait for a security break to happen. As soon as the breach occurs, more information to assess the expected benefits of an information security investment is available, which makes the assessment more accurate" (p. 10).

[2] The attacker behavior is described by the Weakest Link approach, which consists of an ongoing process of locating the least secure element of a system. Ultimately, hackers seek out vulnerabilities and break the weakest link to gain access and entry into a secured environment (Stewart, 2014).

[3] As defined by Howard & LeBlanc (2002), security vectors are externally visible and accessible system resources that can be used to mount an attack on the system and subsequently weighted according to the potential damage that could be caused by any given exploitation of a vulnerability.

1.3 Research Objective

The aim of this thesis is to first, understand the dynamic interactions between defenders and attackers when making information security investment decisions, and second, derive the main implications of two theoretical frameworks from information security investment literature: The Wait-And-See approach for defenders and the Weakest Link approach for attackers. For this purpose, a System Dynamics model is proposed to study investment strategies derived from such theoretical frameworks.

1.4 Research Questions

1.4.1 What are the relevant concepts and variables and relationships described in Wait-And-See and Weakest Link theoretical frameworks?

1.4.2 How can existing theoretical frameworks defined in WAS and WL be represented in a System Dynamics framework?

1.4.2.1 How can the identified concepts and variables in the literature be represented in a stock and flow diagram?

1.4.2.2 Which feedback loops link these concepts and relationships?

1.4.3 What are the dynamic implications of WAS and WL theories in the SD model?

1.4.3.1 How does financial performance for the defender and successful attacks develop over time?

1.4.4 What are the dynamic implications for investment decisions in information security under different uncertainty level scenarios?

1.4.4.1 To what extent does the level of uncertainty of attacks affect investment decisions when capabilities of defenders and attackers are asymmetrical?

1.4.4.2 To what extent does the level of uncertainty of attacks affect investment decisions when security vector values are asymmetrical?

1.4.4.3 Why and under which conditions is it rational for the defenders to under-invest in information security?

1.4.5 What policy options can be identified and what are their dynamic implications?

1.4.5.1 When is it better to defer investments, and respond to attacks in a reactive way?

1.4.5.2 When is it better to move first and take proactive measures?

Chapter 2: Methodology

2.1 Research Strategy and Methodology Choice

This thesis adopts a mixed-methods research strategy. A mixed-methods research strategy combines qualitative and quantitative approaches (Denscombe, 2012). Given that information security is a complex system of many closely interrelated variables as pointed out by Behara et al. (2007), a mixed-methods research strategy is suitable to achieve the objective of this thesis: namely, to understand and derive the dynamic implications between defenders and attackers described by the WAS and WL approaches, respectively. Thus, a dynamic framework within which these approaches can operate with each other over time as they do in the real world, was needed. System dynamics (SD) is a structural theory of dynamic systems (Lane, 1999); it is based on the main hypothesis that the structure of social systems drives system behavior over time and is generally characterized by feedback loops, accumulation processes, and delays between cause and effect.

System Dynamics uses a combination of first-order linear and non-linear difference equations to relate qualitative and quantitative factors within and across time periods and is based on the principles developed by Forrester to study managerial and dynamic decisions using control principles (Forrester, 1961; Homer & Oliva, 2001; Sterman, 2000). In SD, the models are theories about real systems that "must not only reproduce/predict behavior, but also explain how behavior is generated" (Barlas, 1996, p.185-186). Hence, the method employed in this thesis is a qualitative and quantitative System Dynamics modeling and simulation based analysis.

Following the System Dynamics modelling process proposed in the SD literature (Luna-Reyes & Andersen, 2003; Richardson & Pugh, 1981) the qualitative stages to apply in this research are conceptualization and formulation of the model. These stages are helpful to gain insights regarding the complex dynamics between attackers and defenders described in the theoretical frameworks. In the qualitative phase, a systematic literature review was conducted (e.g., De Gooyert, 2016) of information security economics theoretical contributions. Then, the data was collected through a systematic literature review and qualitative SD tools were used to visually represent the concepts found in the literature. The tools to conceptualize the model and to guide the model formulation were stock and flow and causal loop diagrams.

Therefore, the stock and flow as well as causal loop diagrams resulting from the qualitative study, were continued in a quantitative model following modelling phases of model validation and behavior analysis, which provided a "simulations laboratory" enforcing the internal consistency of the theories, thus ensuring that behavior can be generated by its underlying assumptions (Repenning, 2002).

2.2 Data Collection and Analysis

The literature search and selection followed the guidelines of Webster and Watson (2002) who focused on the structure of the literature review and implemented by drawing the steps suggested by Okoli and Schabram (2010) who focused on the process of conducting a systematic literature review. With this in mind, the literature review presented in Chapter 3 of this thesis aims to cover the most relevant existing economic analysis studies of information security investments.

To identify academic papers on the economic analysis of information security investment, a search was conducted for papers in the following databases: ACM Digital Library, Web of Knowledge, EBSCO, Google Scholar, IEEE Xplore Digital Library, Science Direct and the AIS Electronic Library. The search for scientific articles was carried out between February and June 2017 using the search terms "information security investments", "economics of information security", "wait-and-see", "weakest link" and "security decisions". There was no limit for the period of time in this search. In addition, the following search keys were conducted:

- (invest* OR economic OR cost) AND (information OR "information security" OR "information systems") AND ("security process" OR (secure*AND (decision OR "vulnerabilit" OR "vector" OR attacks*OR capabilit* OR performance OR reputation OR "damage")))
- (financ* OR invest* OR cost OR economic) AND "security breach" AND effect,

This search process resulted in a collection of 98 papers. During the collection of the academic papers, a practical screen was applied to determine which papers should be kept for further study (Okoli & Schabram, 2010). Applying the screen was alternated with the literature search in order to limit the amount of work involved in "going backward and forward." A rather tolerant screening was used, since the goal was to obtain a broad overview of the papers published in this domain.

The sample for the scientific articles selected to conduct the qualitative phase of this study was obtained through a qualitative sampling technique, which is better understood as an ongoing iterative process co-occurring with data collection and data analysis (Drisko, 2003; LeCompte & Preissle, 1993). This means that the sample of scientific papers was initially 98 papers as it was the result of the database literature search and then was adapted throughout the process of the literature review. During the screening process, a more elaborate understanding was developed, which resulted in increasingly refined rounds of screening while going through the literature. After the screening process, 45 academic papers remained. The selected articles included economic models for making decisions on IS security investments. Articles with abstracts that did not focus on economics of information security were removed. For example, purely technical articles or which cover only management issues without considering investments in IT security were removed. After this process step, a conceptual stock and flow diagram was built to understand the causes and effects of the main variables of the problem and later, a causal loop diagram (CLD) was constructed to identify the main feedback loops. The SFD and CLD were based on the previous literature review and captured the interactions and relationships between the most important identified variables.

Based on the stock and flow as well as causal loop diagrams that resulted from the previous stage, a quantitative stock and flow model was proposed. The analysis of such model was based on simulations from internally generated data that consequently allows for model validation and behavior analysis under specific scenarios. Simulations aid to discover implications of the theories assumptions that are not intuitively obvious by conducting various tests for model validation, performing sensitivity analysis and scenario analysis in a non-dangerous, non-threatening, non-costly way (Axelrod, 2003; Größler et al., 2008). Thus, the intended tests to be performed in the validation phase are structure tests, structure-oriented tests and behavior tests (see Barlas, 1996). For the behavior analysis stage, the base line scenario will be set based on parameters that generate an equilibrium state between attackers and defenders' strategies, i.e. WL and WAS. The scenario analysis phase, consisted on scenario runs that reflected different levels of uncertainty as well as different conditions for attackers and defender. Finally, the model was used to help to identify and explore policy options to improve the problematic behavior. The purpose of this analysis is an understanding of what policies work and why (Richardson & Pugh, 1981; Sterman, 2000). Policy alternatives were tested through parameter changes and structural changes under the levels of uncertainty examined in the scenario analysis.

Chapter 3: Literature Review

This chapter provides an overview of the literature relevant to this research project to answer the first research question. As mentioned in the previous chapter, the foundations of the qualitative and quantitative data for the system dynamics model constructed for this study, was obtained from the systematic analysis of the literature concerning information security investments. It is important to note that the knowledge gained from the literature review served both as sources of concepts (to form an understanding of the issue) and as sources of estimations and structural knowledge.

3.1 Information Security Investments

To better understand the existing economic analyses of information security investment, the literature was divided into two categories according to their research approaches as classified by Cavusoglu *et al.* (2008): (1) decision-theoretic approach, and (2) game-theoretic approach. The decision-theoretic approach uses the traditional risk or decision analysis framework to determine information security investment level, taking hackers' efforts as exogenous. By contrast, the game-theoretic approach treats information security investment as a game between two players, e.g., between organizations and attackers, in which both the organization's level of security investment level and the hackers' efforts are endogenously determined. Studies in both approaches offer an understanding of how to determine an optimal level of investment in information security and the effectiveness of these investments. Studies in these two areas are described next.

3.1.1 Optimal IS security investment

Studies that investigated the optimal level of information security investment utilized the decision-theoretical and game-theoretical approaches and applied neoclassical economics assumptions.

In previous work, functions of benefit/utility/profit are usually used to describe rational preference. For example, Gordon and Loeb (2002) built a function of expected benefit of information security investment. Their study analyzed the economics of information security investment by comparing the expected benefits of information security investment with the monetary investment in security to protect the given information set.

The results indicate that, for a given potential loss, a firm should not necessarily focus its investments on the information sets with the highest vulnerability. A firm may be better off concentrating its efforts on information sets with midrange vulnerabilities. This study also suggested that for two broad classes of security breach probability functions, the optimal amount to spend on information security never exceeds 37% of the expected loss resulting from a security breach.

In decision-theoretic studies, it is usually assumed that firms will maximize their expected net benefits (e.g., Gordon & Loeb 2002; Shim, 2011; Willemson, 2006, 2010) or profits (e.g., Bohme & Felegyhazi, 2010; Lee et al., 2011). Huang et al. (2008) used a function of expected utility considering a risk-averse firm. Similarly, Kort et al. (1999) develops a model where the firm has the possibility to reduce criminal losses by building up a stock of security capital. The result shows that in the case of the existence of a long-run steady-state equilibrium, the firm fixes its investment in security equipment. In a model extension, Kort et al. (1999) take into consideration a firm's reputation affecting the level of investment in security equipment.

Huang et al. (2006) and Huang & Behara (2013) proposed economic models showing how a firm should allocate its limited security budget to defend against two types of security attacks (distributed and targeted), simultaneously. The result indicates that a firm with a small security budget is better off allocating most or all of its investment on measures against one of the classes of attack; when the potential loss from the targeted attacks and the system vulnerability is relatively large. The firm should allocate most of its budget to prevent such attacks.

There are also risk management analyses based on decision theory (e.g., Bojanc & Jerman-Blažic, 2008b; Hoo, 2000). Huang and Goo (2009) built a general model to manage information security investment and applied the general model to different scenarios of information security, including directed attacks, risk-averse decision makers, and attacker inclination. Their results suggested that the relative size of potential losses is an important factor in determining the level of optimal investment and that the total investment may drop when system vulnerability is high. A risk-averse firm would always invest more than the information security risk but never more than the expected loss. Likewise, Huang (2010) developed a model argued that current economic models of security investment focus on risk reduction as the primary effect of security investments, assuming that they generate no direct business benefit; however, some potential business values, such as brand reputation and data stability, are important considerations in optimizing security investments.

In game-theoretic studies, it is assumed that both players will maximize their payoffs. Cavusoglu et al. (2004) developed functions of expected payoff for both the firm and the hacker. Cremonini and Nizovtsev (2006) and Grossklags et al. (2008) established a function of expected payoff for hackers. When utilizing game-theoretic analyses, it is essential to understand hacker's strategy, however, research shows that it is difficult to determine the rationality of hackers as they may be motivated by a different value system (Wang et al. 2008). In game-theoretic analyses, it is also assumed that players will maximize their profits (e.g., Hausken, 2006; Cavusoglu et al., 2008). On the other hand, in some studies, it is assumed that firms will minimize their costs (e.g., Cavusoglu & Raghunathan, 2004; Bandyopadhyay et al., 2005; Cavusoglu et al., 2005; Liu et al., 2005; Liu et al., 2011).

Complete information is not directly mentioned in decision-theoretical studies. Yet, complete information is implicitly applied in game-theoretical studies, in which the solution to the game involves maximization (or minimization) of a polynomial function. For this to occur, the firm needs to know the hacker's payoff function, and vice versa (e.g., Cavusoglu et al., 2004; Cavusoglu & Raghunathan, 2004; Bandyopadhyay et al., 2005; Cavusoglu et al., 2005; Jonsson & Olovsson, 1997; Leeson & Coyne, 2006; Liu et al., 2005; Gao et al., 2013a, 2013b).

3.1.2 The effectiveness of IS security investment

In the literature, information security investments have been evaluated in terms of their economic effectiveness and efficiency (Kwon & Johnson 2014). There are micro-economic approaches based on game theory (Grossklags et al., 2008; Sun et al., 2008).

The effectiveness of information security investments is usually evaluated in terms of financial metrics based on Return on Investment (ROI) (Gordon & Loeb, 2006; Purser, 2004; Mizzi, 2010; Sonnenreich et al., 2006; Davis, 2005). The term Return on Investment (ROI), which is defined as the calculation of the financial return from an investment based on the financial benefits and costs of that investment, is usually used to refer to the measures of how effectively capital is being used to generate profit. Focusing more closely on investment security, Davis (2005) developed the term of return on security investment (ROSI), which is defined as the calculation of the financial return from an investment in security, such as an initiative or project, based on the financial benefits and costs of that investment. Net Present Value (NPV) and Internal Rate of Return (IRR) are also highly used financial indicators (e.g., Bojanc & Jerman-Blažic, 2008a; Bonjanc et al.,2012; Buck et al., 2008).

Information Security Investment Strategies

There are two particular investment strategies that use both decision theory and game theory principles. This thesis is focused on these investment strategies:

3.1.3 Weakest Link Approach

One key insight from the economics of information security literature is that attackers bent on undermining a system's security, operate strategically (Anderson & Moore, 2006; Cremonini & Nizovtsev, 2006). Moreover, information systems are often structured so that a system's overall security depends on its weakest link (Grossklags et al., 2008; Varian, 2004). Attackers have repeatedly exhibited a talent for identifying the easiest way to bypass a system's security, even when the system's designer remains unaware of the particular weakness (Bohme & Moore, 2009). Bier et al. (2007), use a general game-theoretic setting to study strategic interactions between a single attacker and a defender who optimized the allocation of defenses to multiple targets. Here, the defenders have to cope with uncertainty about an assumed hidden preference of the attacker to target a particular target.

Bohme and Moore (2009) proposed a model for security investment that reflects the interactions between a defender and an attacker. The defender faces uncertainty and repeatedly targets the weakest link. The model explains that underinvestment might reasonably occur when a) reactive investment is possible; b) uncertainty exists about the attacker's relative capability to exploit different threats; c) successful attacks are not catastrophic; and d) the sunk cost to upgrade the defense configuration is relatively small.

3.1.4 Wait-And-See Approach

Firms tend to take a reactive, rather than proactive, approach toward cybersecurity investments related to their organizations according to Gordon et al. (2003). Gordon et al. (2003) suggest that a reactive approach toward the deployment of measures to strengthen cybersecurity beyond some basic minimum may be consistent with an entirely rational economic perspective. The essence of the argument is that, given a fixed amount to spend on cybersecurity measures and uncertainties surrounding security breaches, it may make sense to hold a portion of the budget in reserve and wait for a security break to occur before spending the reserve.

By deferring the decision on spending the reserve, managers may obtain a clearer picture about whether such spending is warranted. In a wait-and-see scenario, actual losses do occur if and when a breach occurs, but the magnitude of those losses may be lower than the expected benefits of waiting, and so on balance, it may well pay to wait. This approach is analogous to the deferment option often discussed in the modern economics literature on capital budgeting (e.g., Pindyck, 1991).

3.2 Literature Review Summary

The following tables summarize the concepts and variables obtained after the literature review. Table 1 presents the main concepts regarding information security investment strategies that will be the base of the interactions between defender and attacker in the system dynamics model. Table 2 shows the identified variables with their cause, effect and their polarity.

Table 1 Relevant Concepts found in the literature of Information Security

Concept	Definition	Source
Reputation	A favorable and publicly recognized name or standing for merit, achievement, reliability etc. In this case, reputation is referred to the public prestige of a company.	(Gordon & Richardson, 2004) (Huang, 2010) (Kort et al., 1999)
Vulnerability	The level of safety that assets of a company possess. It can also be referred as the level of protection of an asset.	(Bojanc et al., 2012) (Cavusoglu et al. (2008) (Gordon & Loeb, 2002) (Huang & Goo, 2009) (Wang et al., 2009) (Willemson, 2006; 2010)
Security Vectors	Security vectors are externally visible and accessible system resources that can be used to mount an attack on the system and subsequently weighted according to the potential damage that could be caused by any given exploitation of a vulnerability Examples of security vectors are: network servers, webpages, e-mail, mobile devices, system configuration, among others.	(Howard & LeBlanc, 2002) (Whitman & Mattord, 2012).
Defenders Capabilities	Available resources to be allocated among assets to increase the level of asset resistance. Once these capabilities are invested in certain asset, these will infer in costs for the defenders.	(Bodin, 2005) (Huang et al., 2006) (Huang & Behara, 2013) (Wang et al., 2009)
Attackers Capabilities	Portion of attackers' resources available to be allocated among defender's assets.	
Fraction of Investment	The portion of capabilities dedicated to protect the company's assets.	(Bandyopadhyay et al., 2005)

		(Bodin, 2005) (Cavusoglu et al., 2004) (Gordon & Loeb, 2002) (Gordon et al., 2003; 2015) (Hausken, 2006) (Huang & Goo, 2009) (Liu et al., 2005; 2011) (Shim, 2011)
Fraction of Attacks	Amount of attacks that attackers distribute among defenders' security vectors in correspondence to the historical successful attacks. Once these capabilities are addressed to certain vector, these will infer in costs for the attackers.	(Anderson & Moore, 2006) Cavusoglu et al (2005) Cavusoglu et al. (2008) Cremonini & Nizovtsev (2006) (Hausken, 2006) (Huang & Goo, 2009) (Jonsson & Olovsson, 1997)
Successful Attacks	Criminal attacks that able to breach defenses of assets through security vectors.	(Bohme & Felegyhazi, 2010) (Bohme & Moore, 2009) (Gordon & Loeb, 2002) (Huang et al., 2008)
Defenders Profit	Monetary gain from increasing the level of resistance of the assets, which in turn increases reputation, thus increasing financial performance.	(Bojanc et al., 2012) (Bojanc & Jerman-Blažic, 2008) (Cavusoglu et al., 2008) (Cavusoglu & Raghnuthan, 2010) (Davis, 2005) (Huang, 2010) (Kwon & Johnson 2014) (Lee et al., 2011) (Mizzi, 2010) (Purser, 2004) (Sonnenreich et al., 2006)
Attackers Wealth	Monetary advantage from breaching defenders' assets.	Cremonini & Nizovtsev (2006) (Grossklags et al., 2008) (Leeson & Coyne, 2006)
Weakest Link Investment Strategy	The weakest link strategy consists on the attacker rationally putting more effort into attacking systems with low security levels. Once the perimeter of an organization is breached, it is often possible for attackers to leverage this advantage.	(Bier et., 2007) (Bohme & Moore,2009) (Cavusoglu et al., 2008) (Grossklags et al., 2008) (Stewart, 2014) (Varian, 2004)
Wait-And-See Investment Strategy	Gordon et al. (2003), present a wait-and-see approach based on real options. The basic idea of their approach is that in case of uncertainty regarding expected benefits, it may be better to wait for key events to occur. As soon as the security breach occurs, more information to assess the expected benefits of a security investment is available, making the assessment more accurate.	(Bohme & Moore, 2009) (Cavusoglu et al., 2014) (Gordon et at.,2003) (Hausken, 2006) (Pindyck, 1991)

Table 2 Identified variables in the literature of Information Security

Cause	Polarity	Variable	Polarity	Effect
Vulnerability in Security Vectors	Negative	**Reputation Building Up**	Positive	Financial Performance of the Defender
Vulnerability in security vectors	Positive	**Reputation Erosion**	Negative	Financial Performance of the Defender
Accumulated Reputation	Positive	**Financial Performance**	Positive	Defender's Profits
Vulnerability in security vectors	Positive	**Successful Attacks (For attackers)**	Positive	Attackers Performance
			Positive	Fraction of Attacks
Vulnerability in security vectors	Positive	**Successful Attacks (For defenders)**	Negative	Reputation Building Up
			Positive	Reputation Erosion
Defender Capabilities	Negative	**Vulnerability in security vectors**	Positive	Successful Attacks
Attacker Capabilities	Positive			
Successful Attacks	Positive	**Fraction of Attacks**	Positive	Vulnerability in security Vectors
Successful Attacks	Positive	**Fraction of Investments**	Negative	Vulnerability in security Vectors
Successful Attacks	Positive	**Attackers Performance**	Positive	Attackers Wealth

Note 1: Positive polarity means that the relationship between the variables amplifying and negative polarity means that the relationship is counteracting.

Note 2: The tables can be read in the following way: The higher Vulnerability in Security vectors, the lower the Reputation Building Up variable. Therefore, the higher Reputation Building Up, the higher the Financial Performance of the Defender.

Chapter 4: Model Description

After the systematic literature review was concluded, a system dynamics model to study the dynamics described in the literature of information security investments, was built. This chapter, together with Chapter 5 aims to answer the second research question. This chapter describes the structure of the system; attention will be placed on providing a model overview and a description of each sub- model. Finally, the overall unified structure of the model will be described in terms of how sectors interact with each other from a feedback loop perspective.

4.1 Model Overview

This section defines the boundary of the model and the major assumptions included in the model. Together, all these elements provide an overview of the model in a way that the reader can understand the operation of the model generally without referring to technical specifications.

As mentioned in previous chapters, the model focuses on the dynamics of the attacker and defender interactions in the information security field to discover the investment strategies applied by the adversaries.

The model presents a firm, that represents the Defender, which is protecting an asset against a set of hackers, representing the Attackers that are trying to breach the security of the firm's asset with malicious cyber-attacks. The asset can take many forms, such as a list of customers, a website, an accounts payable ledger or a strategic plan. The increased security could be with respect to protecting the asset's confidentiality, integrity, authenticity or availability to authorized users.

There exist three possible threats, which can be regarded as distinct security vectors of access of a single asset of the company. Each threat can be secured by investing in its corresponding defense. For each security vector, there is one way to access and one way to defend. Lastly, defenses are effective if they can compensate for the incoming attacks.

As illustrated in Figure 2, the model consists of three sub-models: Defender Sub-model, Battlefield Sub-model and Attacker Sub-model.

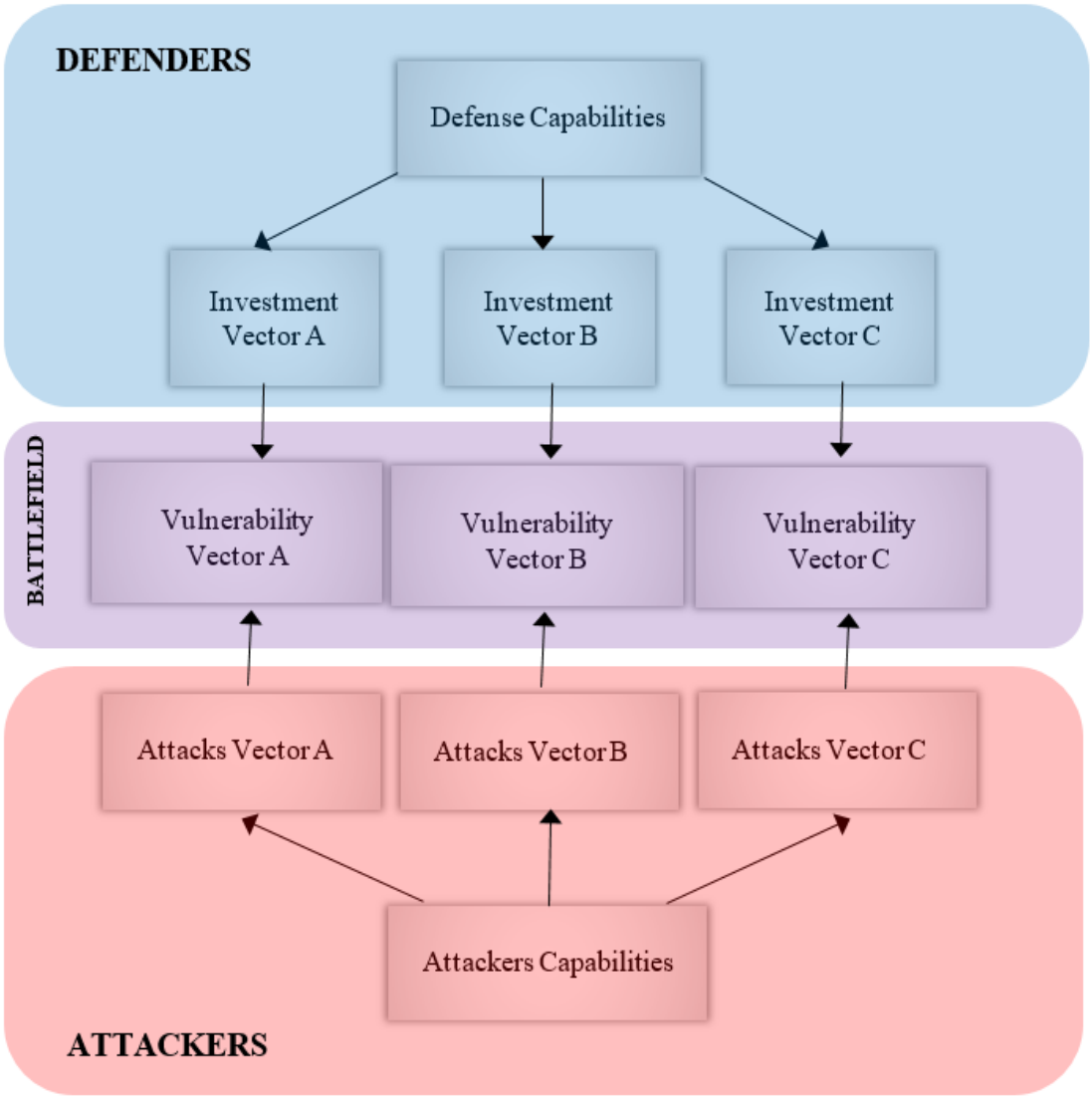


Figure 2 Sub-models Diagram

Using the concept of wargames[4] in organizations known as Red Teaming[5] and Blue Teaming[6] to help differentiate each of the adversaries, this model contains color distinctions for defenders with blue color and attackers with red color. The area where the two opponents interact is called Battlefield and is represented in purple color.

[4] Wargame exercises are akin to Threat Modeling, though geared to the security response process and personnel of an organization or service dealing with an attack. The intent of war gaming is improving security incident response procedures by engaging personnel from different groups inside the organization (Microsoft, 2014).

[5] Red Teaming refers to the use of real-world breach tactics for attack and penetration. Red Teaming takes the theoretical aspect of war-gaming and makes it real (Microsoft, 2014).

[6] The Blue Team follows established security processes and uses the latest tools and technologies to detect and respond to attacks and penetration. (Microsoft, 2014).

4.2 Model Boundary

To gain intuition into the dynamics of attacker-defender interactions, a quantitative and integrative dynamic model with a suitable boundary, time horizon and realistic interpretation of strategic decision making by individuals, is essential.

The model is run in 100 periods representing months, long enough to capture the delayed and indirect effects of the strategies applied by attackers and defenders. Table 3 summarizes the scope of the model by listing and classifying which key variables are included endogenously, which are exogenous and which are excluded from the model.

Endogenous	**Exogenous**	**Excluded**
Reputation	Defenders Capabilities	Type of Attacker
Successful Attacks	Attackers Capabilities	Type of Attack
Vulnerability of Vectors	Attack Unitary Cost	Financial Indicators
Defenders' Financial Performance		
Attackers' Performance		

Table 3 Model Boundary

4.3 Major Assumptions

Assumption 1: Effect of cyber-attacks on the firm's reputation.

There are both direct and indirect costs associated with cybersecurity breaches. The direct costs to companies include the money spent on intrusion-detection systems, overtime for staff fixing compromised systems, and productivity lost during virus attacks, for example. However, these are cost that companies face in the day-to-day operation of their business in an internet world. Although, not perfectly, these costs can be measured by the companies. Direct costs of cyber security, are not considered in this study.

The real financial damage due to cybersecurity breaches comes from indirect costs (Gordon & Richardson, 2004). These can be damages caused by lost sales, weakened customers relationships and legal liabilities. It is difficult to measure indirect costs, but it is worth paying attention to them since they can add up to a substantial impact on a company's revenues.

A company's reputation is fundamental to their economic future. Damage on reputation is considered an indirect cost that a company faces against cyber-attacks. An advertisement, or article containing a security breach, can affect their reputation and financial performance. An example of this is a virus attack to a bank's ATMs causing them to shut down for a few hours, this may bother the customers, but they will probably not change banks over such an incident. Nonetheless, if a bank is hacked and customer data is circulated on the internet, customers may well decide to take their business elsewhere. In the latter case, the breach has marked negative impact of the reputation and therefore on the market value of the company because of the real potential for lost future revenue as customers choose to change banks (Kiely & Benzel, 2006).

This model assumes a value for each of the three vector of security as the weight they place on their reputation, together with the status of the vectors vulnerability and successful attacks. Simulations will provide insight into the value a company places on cyber security in regard to preserving their reputation.

Assumption 2: Capabilities of defenders and attackers are exogenous parameters.

A firm's ability to invest in information security, or everything else for that matter, is limited by its finances. In particular, information security has to compete with other projects for funding (Tipton & Kreuse, 2006). Given the budget limitations, the greater challenge to managing information security is not so much the total of investment level needed, but the allocation of the finite resources to defend against attacks (Huang & Behara, 2013).

In general, large companies a specified budget to take care of security incidents. Then, depending on the size of the company and the type of industry it belongs to, the capabilities of firms will differ. This model assumes a relatively big-sized company since the budget for information security is independent of the firm's financial performance. In other words, the budget dedicated to invest in information security, in this case, is fixed and available for every period of the simulation.

The attackers' capabilities are also assumed to be constant for each period. In the real system, hackers are criminal organizations who operate under their own business model. Consequently, it is not known how exactly the attackers behave and on what they build their business case and, in this case, how they shape their resources for future attacks. The model here reflects the reviewed literature concerning attackers' behavior and capabilities.

Assumption 3: Attack Unitary Cost

The attack unitary cost denotes the ratio between attackers' and defenders' capabilities. This parameter represents the damage that each fraction of attack causes to the defenders' performance. In other words, the attack unitary cost is how much money it takes for the defender to stop an attack.

In the model, the attack unitary cost is exogenous. This parameter will be multiplying the attackers' capabilities in order to determine the vulnerability status of each security vector.

Assumption 4: Type of Attackers and Type of Attacks

Cyber-attacks can originate from inside or outside the company. The model does not differentiate between internal attackers and external attackers. Internal attackers include disgruntled employees and negligent employees who employ a weak password for accessing the system or click on a link from a phishing site without knowing it is a malware. The other type of attacker is external which in general, include criminal activist hacking organizations. Instead, attackers in this model are identical and there is an unspecified number of them.

In addition, the model does not parse the attacks into different types, e.g., denial of service, phishing, virus, ransomware, SQL injections and so on.

Assumption 5: Security Cost of Defenders

In this study, the security cost that the defenders incur when making an investment decision each period is portrayed in the decision rule of the fraction of investment they dedicate to each security vector when this is breached.

However, what is not depicted in the model, are different financial indicators and approaches to analyze each investment decision such as: Cost-benefit analysis, risk analysis, Net Present Value (NPV), Annual Loss Expectation (ALE), Return of Security Investment (ROSI), among others. The reason for this, is that a financial analysis would require a more sophisticated model including empirical evidence to give more accuracy to the research. Additionally, the time constrains compels this theoretical study to exclude financial analysis.

4.4 Model Structure

4.4.1 Stock and Flow Diagram

In the case of quantitative system dynamics modelling, stock and flow diagrams are the tool by which model structure is defined, represented and evaluated. Model structure from a system dynamics perspective can be defined as the set of stocks, flows and auxiliary variables by which the representation of any system is achieved.

Stocks are variables in which quantities accumulate over time, these are represented by rectangles. Flows are the variables affecting stocks and through which accumulation or depletion of stocks occur and are represented by arrows and valve symbols (Forrester, 1961). Stocks accumulate (integrate) their inflows less their outflows. Thus, a stock and flow map corresponds to a system of integral or differential equations. Units of measure can also help identify stock and flows. If a stock is measured in units, its flows must be measured in units per time period (Sterman, 2000).

Auxiliary variables serve either to represent external parameters (parameters outside of the system's influence) or as the intermediate steps by which stocks and flows affect each other through feedback mechanisms to add conceptual clarity to the model (Richardson & Pugh, 1981; Sterman, 2000).

Model structure represents both the qualitative dimension of the system, through the causal linking of variables, and its quantitative dimension, through the formal definition of these causal links through equations. The complete documentation of the model, including all equations, variable units, and reference to the source of estimated values as well as general notes of some formulations, is presented in the Appendix.

As shown in Figure 3, the system dynamics model contains three sub-models:

- Defender Sub-model
- Battlefield Sub-model
- Attacker Sub-model

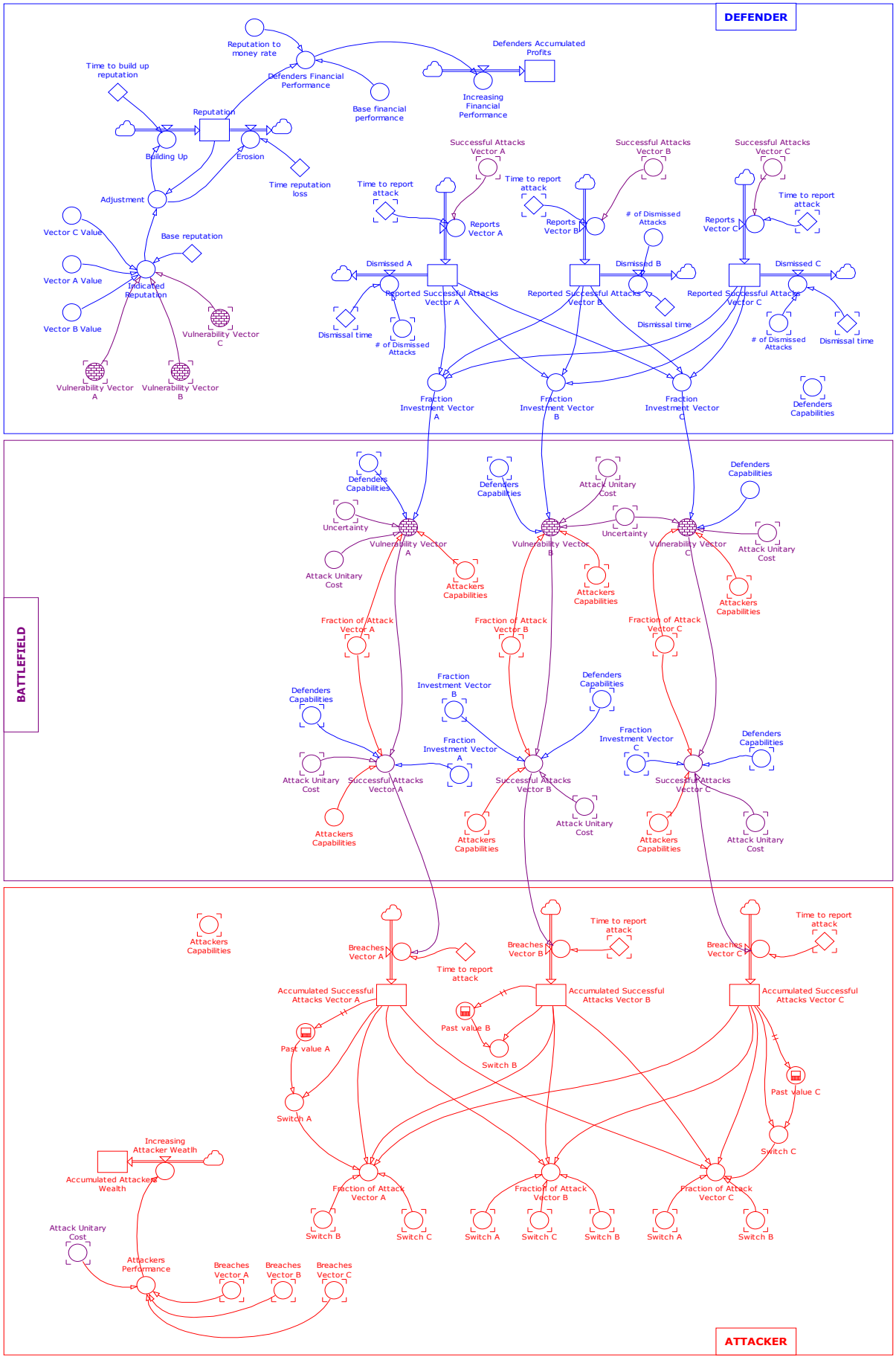


Figure 3 Complete Model Architecture

4.5 Sub-models Description

The following section describes the structure of each sub-model in terms of stock and flows and main formulations.

4.5.1 Defender Sub-model

Figure 4 illustrates the Defender Sub-model structure. This sub-model represents the firm's defense structure against malicious cyber-attacks that are trying to breach the security of its information asset. In each period, the defender makes a security investment decision to define his configuration of defenses. Defenders are assumed to have a basic security on each vector and their security capabilities are destined to cover the additional security efforts resulting from security breaches.

As shown in this figure, the defender is protecting his asset through three security vectors (A, B and C), which have a value that will be translated into reputation and afterwards to financial performance. In the model, the security vectors are represented as each vector's vulnerability status.

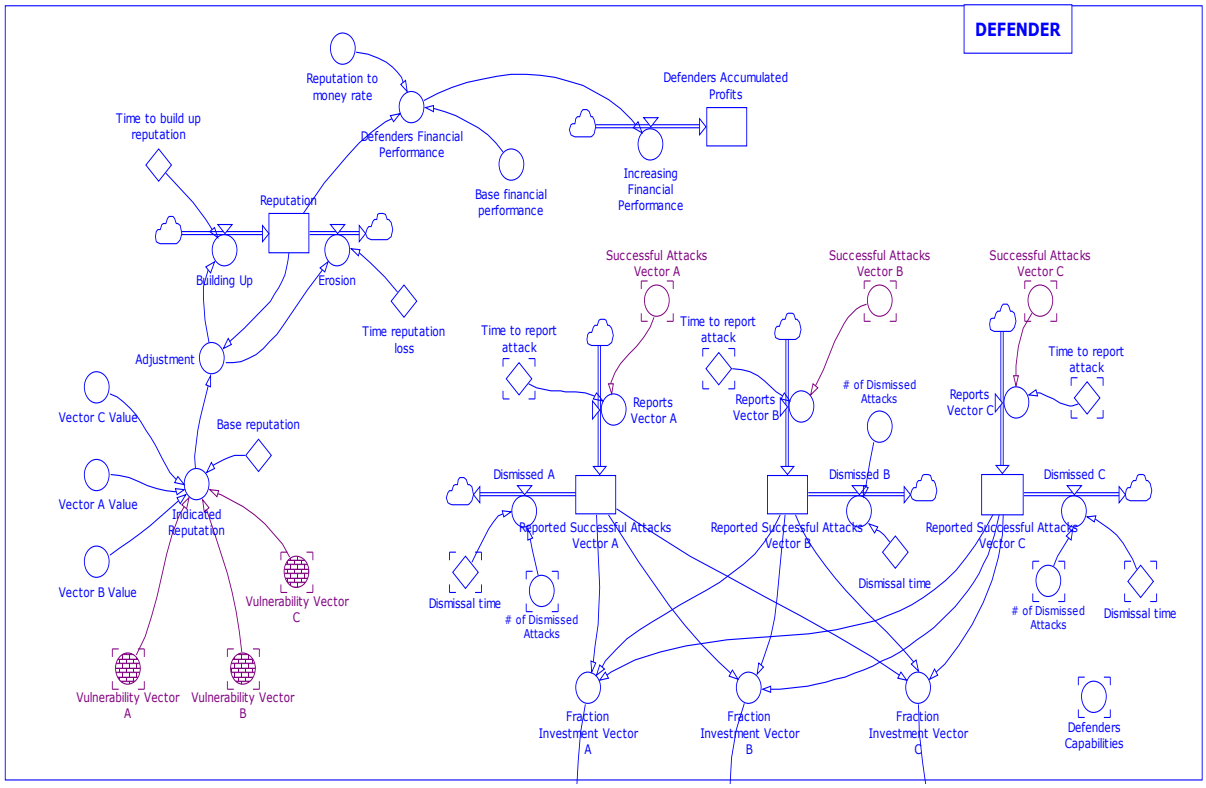


Figure 4 Defense Sub-Model Structure

Reported Successful Attacks

There are three stocks of reported successful attacks, one for each security vector symbolized by the notation *i* to represent vectors A, B and C.

Stock: *Reported Successful Attacks*$_i$

Init: *A constant number, they are initialized in 5 Attacks*

Inflow: *Reports= Successful Attacks/Time to report Attack*

Outflow*: Dismissed= Number of Dismissed Attacks/Dismissal time*

Each stock has an inflow of successful attacks on that specific vector, per the time it takes to the defender to report successful attacks (1 month). The outflows of these stocks are the number of dismissed attacks that were reported divided into the time it takes for defenders to dismiss such attacks (1 month). The model was calibrated to determine the value of 3 as an assumed constant number of attacks to be discarded every period.

Fraction Investment Vectors

The fraction of investment for each vector is calculated by the reported successful attacks divided into the sum of the reported successful attacks of all three vectors. The following equation is an example of the Fraction of Investment formulated of the defense in Vector A and it is the same formulation for the other two vectors.

Fraction Investment Vector A*= Reported Successful Attacks Vector A/ (Reported Successful Attacks Vector A+Reported Successful Attacks Vector B +Reported Successful Attacks Vector C)*

This equation dictates that the defender will invest a percentage in vector A which is equal to the total successful attacks he has received on that vector.

Reputation

Reputation is represented as a stock that accumulates in Reppoints over the course of each simulation period. The inflow of reputation is the Building Up rate derived by an adjustment of reputation which is in turn the result of the sum of the values of each security vector and their respective result of vulnerability on each vector.

Stock: Reputation

Init: *A constant number, it is initialized in 50 reppoints*

Inflow*: Building Up= IF(Adjustment>0, (Adjustment/Time to build up reputation),0)*

Outflow*: Erosion= IF (Adjustment<0, (ABS (Adjustment/'Time reputation loss)),0)*

The initial value of the stock is 50, being this number the current reputation that the firm has in the beginning of the simulation period. What this inflow represents is the following decision rule: reputation building up rate will increase, whenever the adjustment is positive. In contrast, when the adjustment is negative, the outflow of erosion will increase, meaning that the firm is losing reputation.

Adjustment*= Indicated Reputation-Reputation*

The adjustment is the gap between the indicated reputation and the current reputation of the company. The adjustment will be determined by the result in indicated reputation, which is a linear funcion of the vectors vulnerability, being the base reputation (100 reppoints) the intercept of this function.

Indicated Reputation*= Base reputation-(Vector A Value*Vulnerability Vector A+Vector B Value*Vulnerability Vector B+Vector C Value*Vulnerability Vector C)*

Defenders Financial Performance

The defenders' financial performance is formulated by the sum of the current reputation per the reputation to money rate, which indicates how much the reputation points are worth in money, plus the base financial performance of the firm (50 Euros).

Defenders Financial Performance*= (Reputation to money rate*Reputation)+Base financial performance*

The Defenders' Profit is given by the financial performance; this stock was built for analysis purposes in the following scenario and policy options analysis.

Stock: *Defenders Accumulated Profit*

Init: *A constant number, it is initialized in 0 Euros*

Inflow*: Increasing Financial Performance= Defenders Financial Performance*

4.5.2 Battlefield Sub-model

The Battlefield Sub-model is the segment of the model where defenders and attackers interact with their respective capabilities and investment decisions. The main components of this sub-models are Vulnerability and Successful Attacks of each security vectors. Figure 5, depicts the battlefield sub-model:

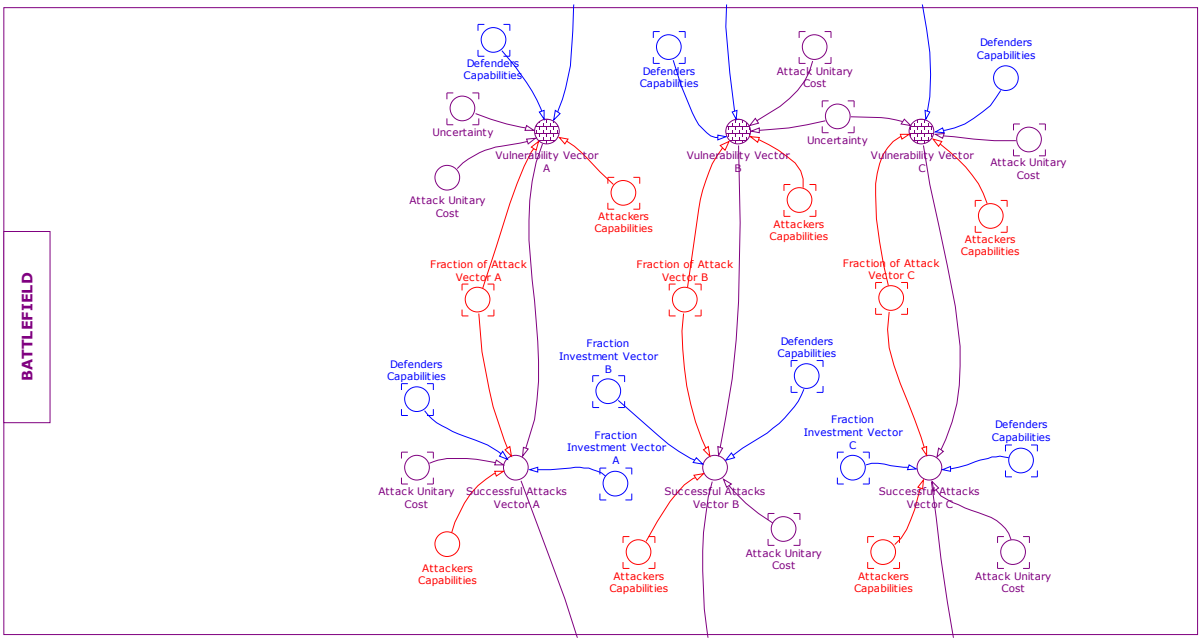


Figure 5 Battlefield Sub-Model Structure

Vulnerability in Vectors

Vulnerability stands for the level of security in place on each vector. If the vulnerability is positive, it means the system is weak in security. Vulnerability is calculated by:

Vulnerability Vector A*= (Attackers Capabilities*Fraction of Attack Vector A*Attack Unitary Cost)-(Defenders Capabilities*Fraction Investment Vector A)*

Vulnerability Vector B*= (Attackers Capabilities*Fraction of Attack Vector B*Attack Unitary Cost)-(Defenders Capabilities*Fraction Investment Vector B)*

Vulnerability Vector C*= (Attackers Capabilities*Fraction of Attack Vector C*Attack Unitary Cost)-(Defenders Capabilities*Fraction Investment Vector C)*

Basically, vulnerability is defined by the difference between the resources that the attacker destines for the correspondent vector and the resources the defender allocates to fix security flaws in the same vector. The attacker's resources are given by his capabilities per the fraction of capabilities dedicated to attack the vector per the money to attack equivalent for each attack. Similarly, the defender's resources result from multiplying his capabilities and fraction destined to defend the vector once breached.

Successful Attacks in Vectors

The successful attacks are essential to this model since they will trigger the future investment decisions for both adversaries. Successful Attacks are calculated by:

Successful Attacks Vector A= IF(Vulnerability Vector A>0,(('Attackers Capabilities*Fraction of Attack Vector A)-((Defenders Capabilities*Fraction Investment Vector A)/Attack Unitary Cost)),0)

Successful Attacks Vector B= IF(Vulnerability Vector B>0,(('Attackers Capabilities*Fraction of Attack Vector B)-((Defenders Capabilities*Fraction Investment Vector B)/Attack Unitary Cost)),0)

Successful Attacks Vector C= IF(Vulnerability Vector B>0,(('Attackers Capabilities*Fraction of Attack Vector C)-((Defenders Capabilities*Fraction Investment Vector C)/Attack Unitary Cost)),0)

This formulation entails that if the vector vulnerability is lower than zero, then there will be zero successful attacks since the defender has equal or superior capabilities than the attacker and he is capable to stop all attacks. On the other hand, if the vector vulnerability is higher than zero, there will be successful attacks.

The multiplication of defender's capabilities per the fraction of investment and then divided into the attack unitary cost, suggests the amount of attacks that the defender can stop whenever a security breach happens. So, the difference between the number of attacks addressed to each vector and the number of attacks the defender is able to halt from breaching the defenses, is equal to the total successful attacks.

4.5.3 Attacker Sub-model

The attacker sub-model is simple. An attacker targets this firm and puts a certain amount of effort into attacks. Since, the attacker does not know where to aim in order to get benefits, he sends an initial attack distribution according to what is it initially perceived to be vulnerable.

The attacker identifies and exploits the weakest link, that is, the security vector with the lowest protection. If the attacker succeeds, he profits, which will mean lower financial performance for the defender. The attacker does not operate indiscriminately, rather he only attacks when it is profitable to do so.

Historical successful attacks in the attacker's model, encourages to attack the weakest link and do not neglect the other vectors, assigning a smaller portion of resources to attack those. It is assumed that the attacker receives the same utility for exploiting all security vectors.

The following figure illustrates the structure of the attacker's sub-model:

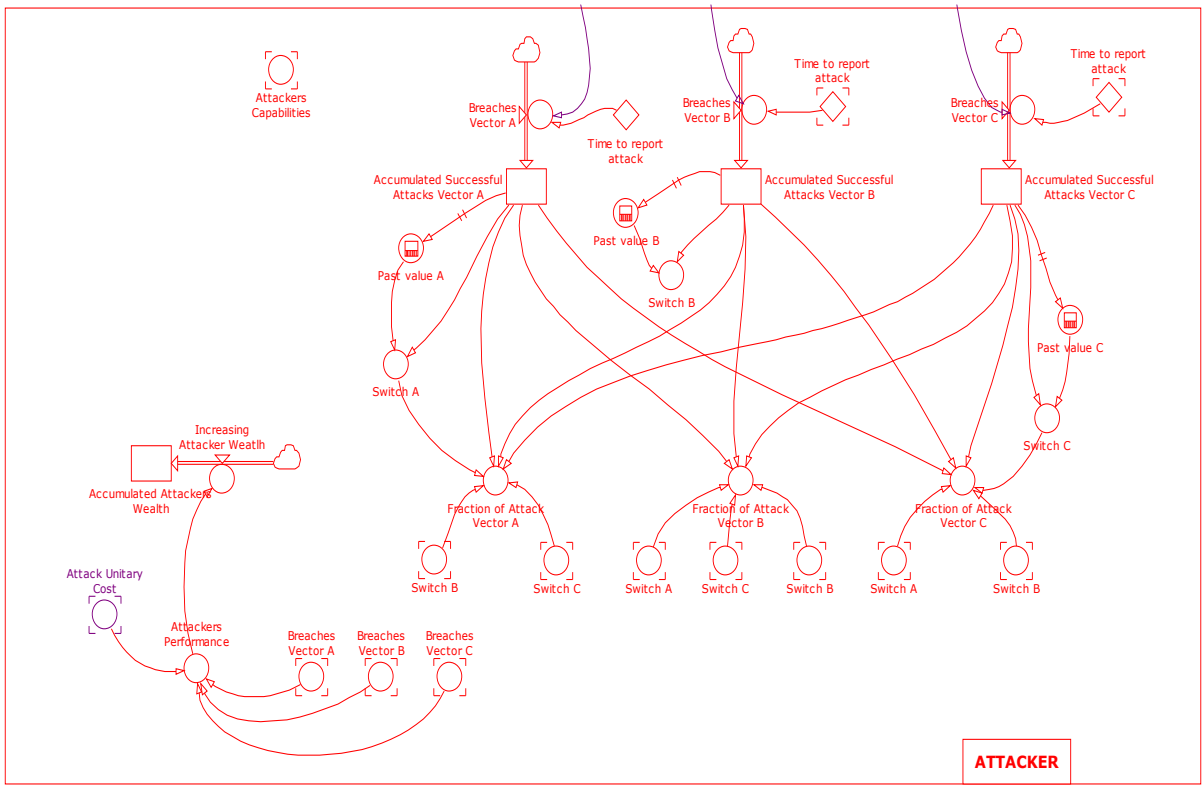


Figure 6 Attacker Sub-Model Structure

Accumulated Successful Attacks

The stock of accumulated successful attacks of each vector, allow the attacker to identify the weakest link and determine the next attack decisions to exploit the most vulnerable security vector. The notation i, indicates Vectors A, B and C.

Stock: *Accumulated Successful Attacks Vector i*

Init*: A constant number, they are initialized in 5 Attacks*

Inflow: *Breaches= 'Successful Attacks Vector i/Time to report attack*

The inflow of this stock is given by the successful attacks in vector *i*, divided into the time it takes attackers to report attacks (1 month).

Fraction of Attack Vectors

The fraction of attacks are the decisions attackers make resulting from the accumulated successful attacks on each vector. In order for the weakest link strategy to operate in this model, attackers have to switch from one vector to the other when the current vector is not being beneficial enough for him to stay attacking it.

For this reason, the past value parameter is in place to store the previous value of the previous period to be able to compare the current value of the attack with the past value of the accumulated successful attacks in the last period and determine if it is increasing or decreasing to make the decision of changing vectors or not.

Past Value*= DELAYPPL(Accumulated Successful Attacks Vector i,1,0)*

Switch*= IF(Accumulated Successful Attacks Vector i-Past value i<1,0,1)*

The switch parameter is a conditional that indicates that when the comparison of current value with past value is lower than 1, then the switch becomes zero and it is not beneficial for the attacker to continue exploiting that vector and jumps to another one. The conditional is towards 1 and not zero because 1 is a threshold to evaluate the different between the two values that must be at least equal to one to justify the change.

This is an example of the calculation of the Fraction of attack of Vector A, however is the same for the rest of the vectors:

Fraction of Attack Vector A*= Switch A*Accumulated Successful Attacks Vector A/(Accumulated Successful Attacks Vector A+Switch B*Accumulated Successful Attacks Vector B+Switch C'*Accumulated Successful Attacks Vector C)*

Whenever an attacker makes the decision to stop attacking one vector and swith to another, then the investment directed to the other two vectors will increase.

Attackers Performance

The attackers' performance is the sum of the breaches of all vectors and multiplied by the attack unitary cost:

Attackers Performance*= ((Breaches Vector A) +(Breaches Vector B)+('Breaches Vector C))*Attack Unitary Cost*

The Attackers Wealth is given by the financial performance; this stock was built for analysis purposes in the following scenario and policy options analysis. The inflow of the attackers' wealth is a function of the attackers' performance.

Stock: *Accumulated Attackers Wealth*

Init: *A constant number, it is initialized in 0 Euros*

Inflow*: Increasing Attackers Wealth = Attackers performance*

4.6 Feedback Analysis

This chapter provides a general description of the model in terms of its main feedback loops. Richardson & Pugh defined feedback "as a closed sequence of causes and effects, that is, a closed path of action and information" (1981, p. 4). All dynamics arise from the interactions of two types of feedback loops: reinforcing loops (R) that amplify whatever is happening in the system and balancing loops (B) that counteract or oppose changes.

Feedback is one of the fundamental concepts of System Dynamics. However, humans have cognitive capacity limitations, thus, mental models often fail to include the critical feedbacks determining the dynamics of systems (Forrester 1992; Vennix, 1996). System dynamics uses diagramming tools to capture the structure of systems, including causal loop and stock and flow diagrams.

Causal loop diagrams (CLDs) are an important tool for representing the feedback structure of systems (Coyle, 2000; Wolstenholme & Coyle, 1983). CLD is a representation that consists of variables connected by arrows denoting the causal-and-effect relationships among the variables (Coyle, 2000; Richardson, 2013). Causal relationships support the clarification of the actual structure of the examined problem, as the clear picture of the problem's structure improves understanding of the observed phenomena (Forrester & Senge, 1980).

CLDs are commonly used in academic work and in business for: system boundary definition, eliciting and capturing the mental models of individuals or teams, communicating the important feedbacks responsible for a problem, raising awareness about unexpected consequences and identifying policy levers (Sterman, 2000). A causal diagram consists of variables connected by arrows denoting the causal influences among variables. The arrows with two lines denote some delays between two linked variables. Each causal link is assigned a polarity, either positive (+) or negative (-) to indicate how the dependent variable changes when the independent variable changes. Note that the loop identifier circulates in the same direction as the loop to which it corresponds.

To simplify the model's representation of the dynamic hypothesis, a causal loop diagram (CLD) was built and it is shown in Figure 7. Loops representing Defenders' actions are represented in blue color and loops for attackers in red color.

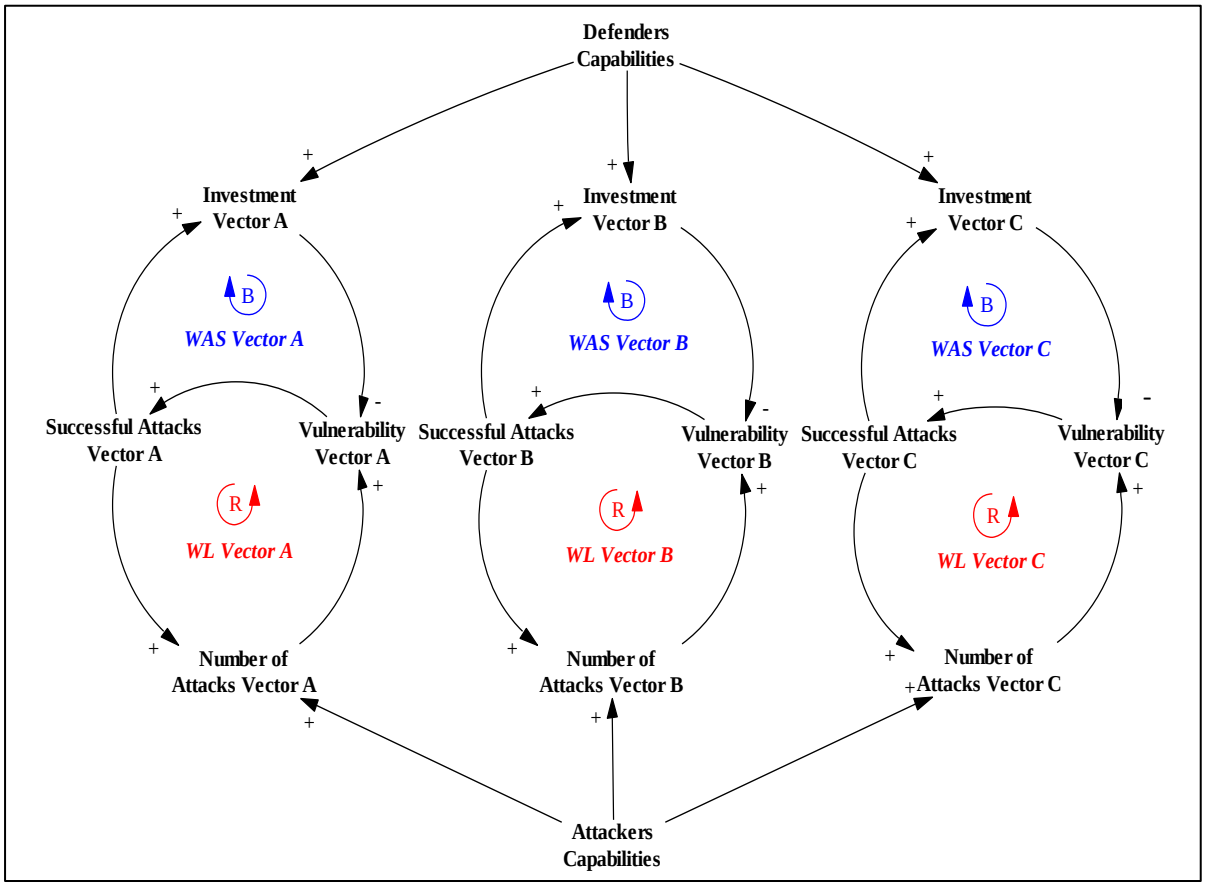


Figure 7 CLD of Defender-Attacker dynamic interactions in Information Security Investments

The core structure (or the main causal loops) of the model is based on the dynamic interactions between the actions of the attackers and the target firm (defenders), influencing and influenced by factors as, capabilities, perceived benefits, and perceived ease of attack (Cremonini & Nizovtsev, 2006; Jonsson & Olovsson, 1997; Leeson & Coyne, 2006).

Each process in this CLD, is common to numerous literature of the Wait-And-See (WAS) and Weakest Link (WL) approaches and each link has support from empirical studies (Gordon & Loeb 2002; Gordon et al. 2003; Varian, 2004; Bohme & Moore, 2009). The novelty of this framework arises from the combination of these approaches to describe the complex interactions of defenders (companies) and attackers (hackers) when making investment decisions on security vectors A, B and C.

As the figure illustrates, important model variables and the causal relationships among these variables are linked by arrows with polarities. In this CLD, there are three reinforcing loops and three balancing loops, one pair for each security vector.

The main feedback loop is a reinforcing one, that is, the Weakest Link loop where the successful attacks lead to more attacks. Although those dynamics is plausible, the implied result of zero or infinite number of attacks from this reinforcement is unrealistic. Constraining such a reinforcing loop, the firm's investments in information security and the effectiveness of such investments, takes place as the Wait-and-see loop. Next, these two main feedback loops will be explained individually.

The **Weakest Link loop** for security vector A, B and C. These are the actions that a rational attacker take when planning the number of attacks to address to defenders' asset. The higher the vector's vulnerability, the higher the successful attacks. The vector's vulnerability will be determined by the ratio between the defenders' capabilities and attackers' capabilities. As successful attacks increase, there will be more number of attacks on vectors will increase as well. Therefore, the higher the number of attacks, the higher the vector's vulnerability will be because the vector will be overloaded with attacks, therefore, making it more vulnerable.

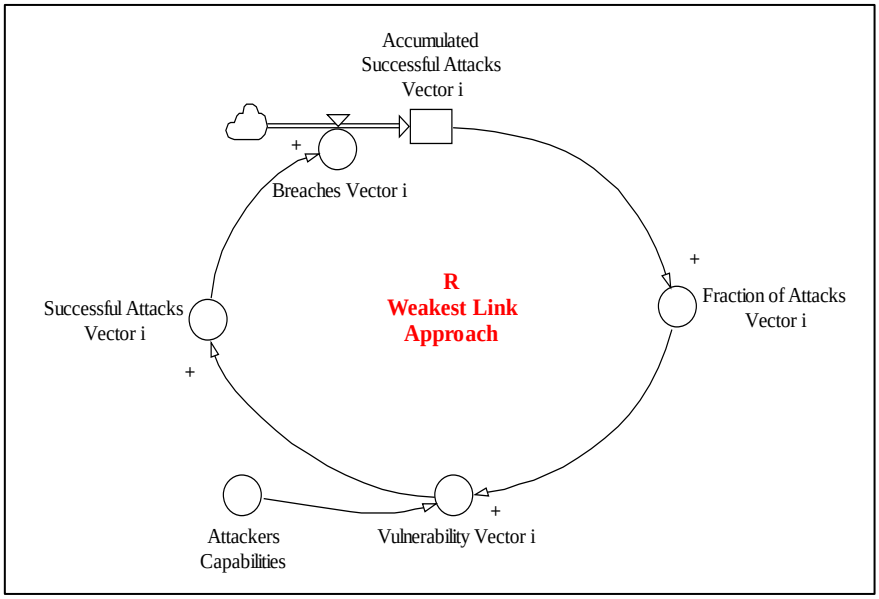


Figure 8 Weakest Link Loop

As shown in Figure 8, whenever there is a weakest link identified, the attacker will focus on the least protected, dedicating less resources to the other vectors. The attacker will not stop attacking the other two vectors, instead, she will continue attacking them in lower proportions in case, another weakest link is found. This happens because the attacker expects that the defender will reduce the vulnerability of the vector, eventually.

On the other hand, the **Wait and See loop** for vector's A, B and C operates when defenders make investment decisions based on their reported successful attacks. The higher the successful attacks, the higher the investment on vectors' security. The more investment, the more level of security of assets, thus, the lower the vulnerability to attacks. Therefore, the lower the successful attacks.

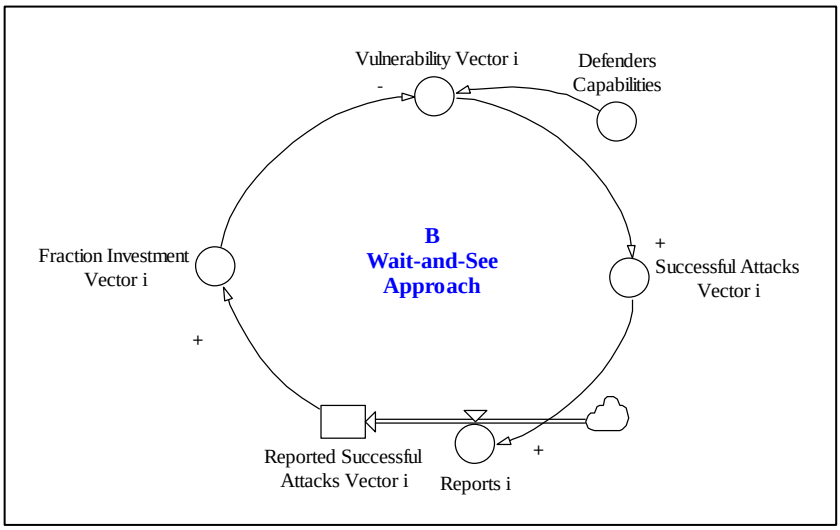


Figure 9 Wait-and-see Loop

Figure 9, illustrates how defenders allocate their resources whenever the weakest link is exploited. This means the defenders is acting reactively to attacks and trying to fix the flaws in security of each vectors. However, as attackers do, even if defenders focus most of their investment in the vector that is being attacked the most, they still protect the other two assets but in lower proportions. The fraction of investment of the other non-weakest link vectors will depend on the amount of attacks these are receiving.

Effect of vulnerability in financial performance of Defenders and Attackers

The result of the vulnerability of the vectors will translate into reputation, which will improve or worsen the defender's financial performance.

The higher the vulnerability of vectors, the lower the reputation of the firm. Therefore, the lower financial performance and profits. The same happens for attackers, an increase in vulnerability leads to an increase in attackers' wealth.

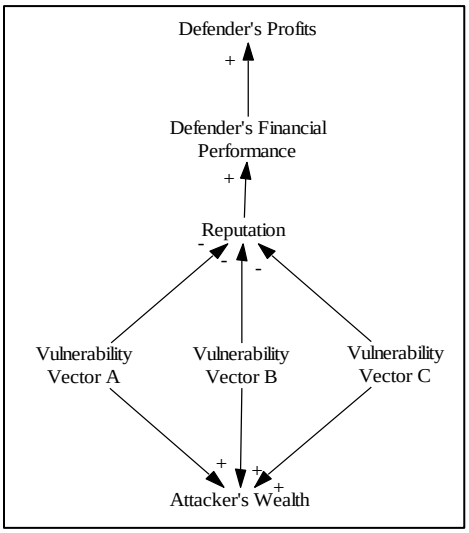


Figure 10 Effect of Vulnerability in Financial Performance

Chapter 5: Behavior Analysis

The model behavior is depicted in this chapter, answering the second research question. The simulations resulting from the base run and equilibrium run are shown and analyzed. The behavior analysis is an essential part of this study since it will be the basis simulation to later validate the model and to explore the scenarios and policy options. The model was constructed in Powersim Studio Software, version 9. The simulation specifications are the following:

- Integration Method: Runge-Kutta (4^{th} order)
- Time Unit: Months
- Time Step: 0.25
- Time Horizon: 100 months

5.1 Base Run

The baseline run is the model simulation in "Business-as-usual" state. The weakest link mechanism is the one that triggers the investment strategies both for attackers and defenders, since also defenders need to identify where is the weakest link in their vectors to decide where to invest and how much. The weakest link mechanism operates under initial conditions reflected in the accumulated successful attacks in the attackers' sub-model.

The initial conditions on the attackers accumulated successful attacks will set the subsequent actions for both adversaries. Whenever there is one security vector breached in the defense, considerably higher than the other vectors, there will be exploitations by the attackers. For the base run, the initial conditions for accumulated successful attacks are:

Accumulated Successful Attacks Vector A	10
Accumulated Successful Attacks Vector B	7
Accumulated Successful Attacks Vector C	5

Table 4 Base Run: Accumulated Successful Attacks Initial Conditions

In this case, vector A is the clear weakest link identified by the attacker in the first period. These initial values were selected this way, to visualize the preference that the attacker has for one of the vectors in comparison with the rest. However, there is a second-preferred vector (Vector B) to show the proportion of the attackers' capabilities dedicated to each of the vector's successful attacks.

The key variables considered in the baseline simulation runs are Successful Attacks (A, B, C), Security Vectors (A, B, C), Investment/Attack in Security Vectors (A, B, C), Defenders and Attackers Performance.

Successful Attacks for all three vectors are portrayed in Figure 11. An interesting observation can be pointed out in this graph, as it exhibits the switches from one vector to the other in attack fraction that the attacker concentrates as soon as another weakest link is spotted over time.

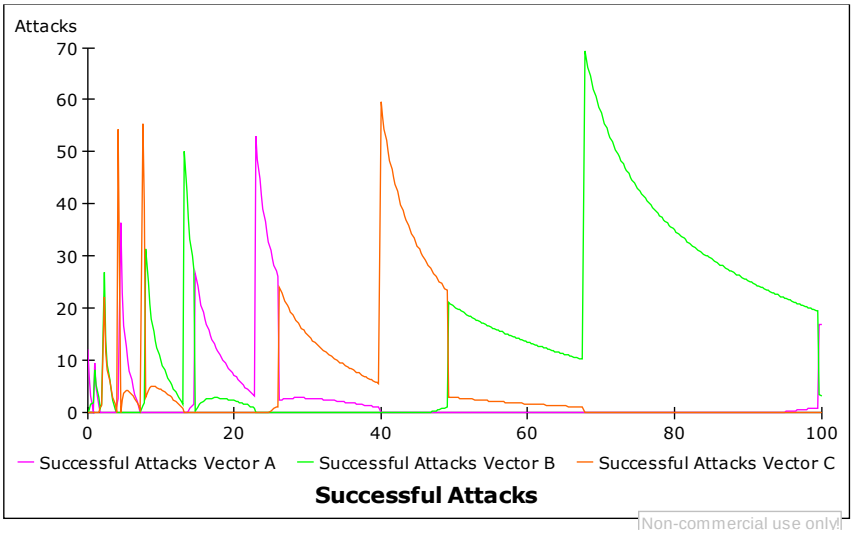


Figure 11 Base Run: Successful Attacks

Simultaneously, as successful attacks happen, the vulnerabilities in vector A, B and C are also changing according to the interactions of Attackers and Defenders. This means that when the attackers capabilities outweigh the defenders' capabilities, the vulnerability in the vector that is most fired upon will experience a positive vulnerability or negative security level. The following figure illustrates the performance of each security vector over time.

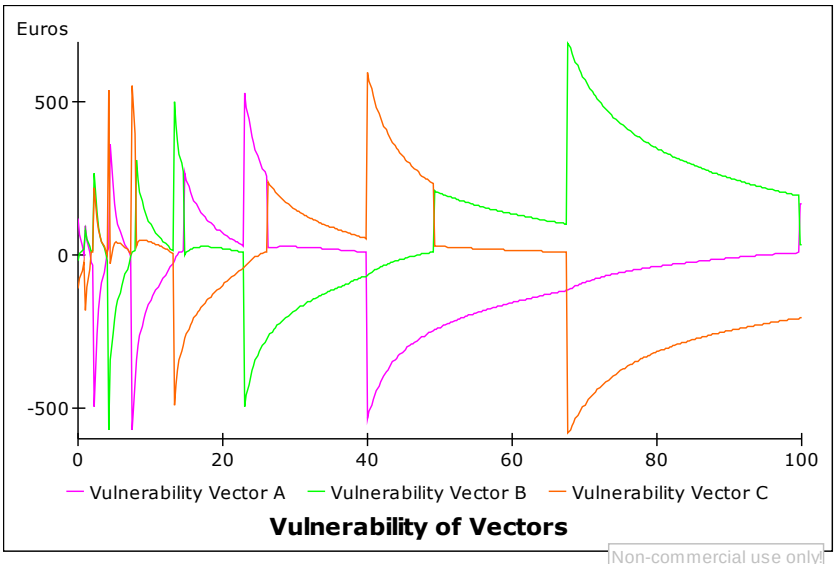


Figure 12 Base Run: Vulnerability of Vectors

To understand deeper the dynamics of the investment decisions executed by both adversaries when the weakest link mechanism is activated, the following figure shows how Attackers and Defenders operate per their respective capabilities. The dynamics of these interactions are depicted in Figure 13.

When the attacker identifies the weakest link in the defense, she will leverage that advantage until there is no more benefits to take out from there, meanwhile the defender fixes the security gap taking a wait-and-see approach, forcing the attacker to change to another target in the following periods.

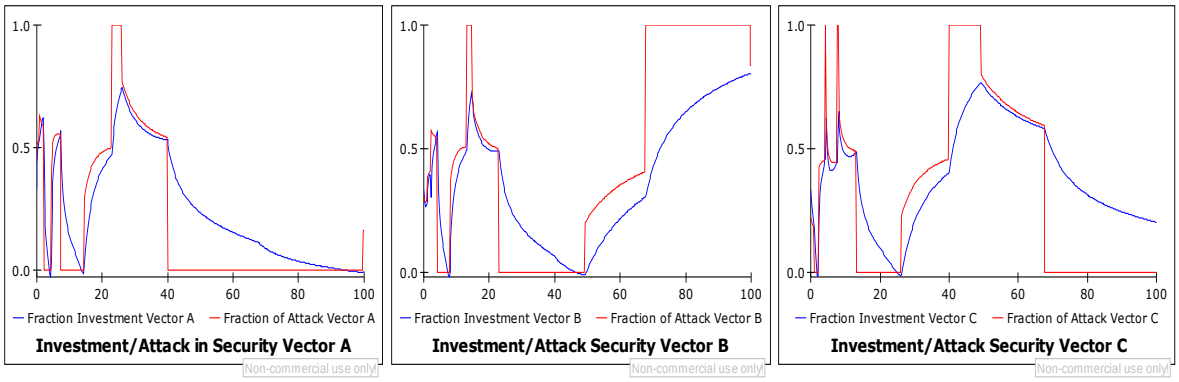


Figure 13 Base Run Investment/Attack in Security Vectors

Figures 14 and 15 show the defenders and attackers financial performance in the base run. It is clearly seen that in this case, both adversaries are increasing their monetary gains. However, defenders are able to defend their information asset effectively even though attackers are being successful at attacking the weakest link in the security vectors.

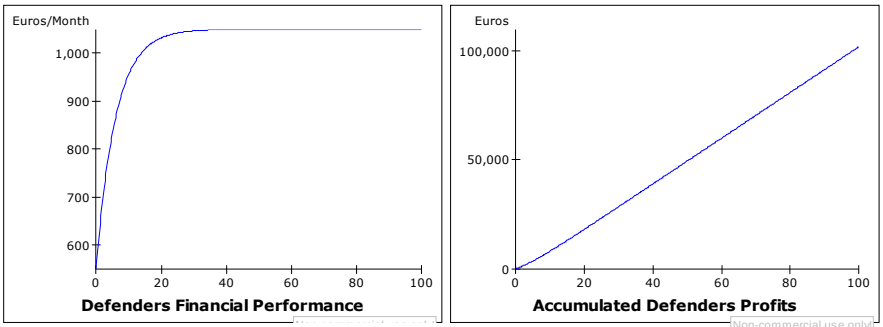


Figure 14 Base Run: Defenders Performance

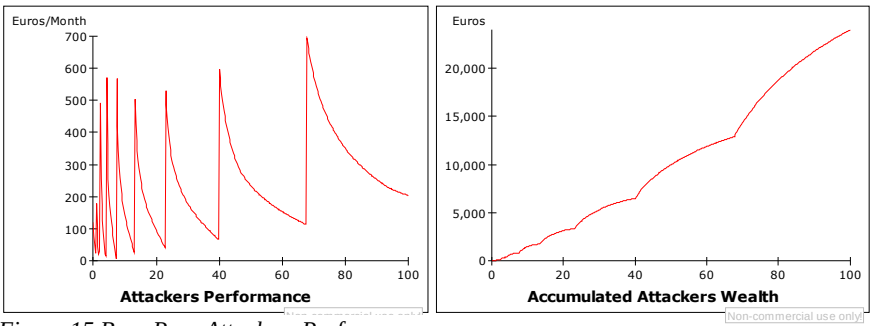


Figure 15 Base Run: Attackers Performance

5.1.1 Dynamic implications of the Base Run

The system behavior in the base run exhibited the weakest link and wait-and-see strategies operating with initial conditions of accumulated successful attacks Vector A= 10, Vector B=7 and Vector C= 5. It was observed that attackers are constantly finding the weakest link and exploiting it (Vector A). Then the attacker switches to the next weakest link whenever the defender blocks attacks, eventually.

Meanwhile, defenders are fixing the defense flaws proportionally as the attacks happen on each vector. The financial performance of both defenders and attackers is visualized while each party is applying their investment strategy, as well as the status of the vulnerability of vectors.

5.2 Equilibrium Run

The equilibrium run differs from the base run simulation by introducing identical values to the accumulated successful attacks for attackers preventing them to apply the weakest link approach. For the equilibrium run, the initial conditions for accumulated successful attacks are:

Accumulated Successful Attacks Vector A	5
Accumulated Successful Attacks Vector B	5
Accumulated Successful Attacks Vector C	5

Table 5 Equilibrium Run: Accumulated Successful Attacks Initial Conditions

These initial values were introduced to portray the situation when there are no successful attacks because the amount of accumulated successful attacks from the attacker's side and reported successful attacks are the same.

The following figures represent the equilibrium run where attackers and defender's capabilities are the same, there are no successful attacks because attackers do not find the weakest link and defenders are able to protect their information asset effectively.

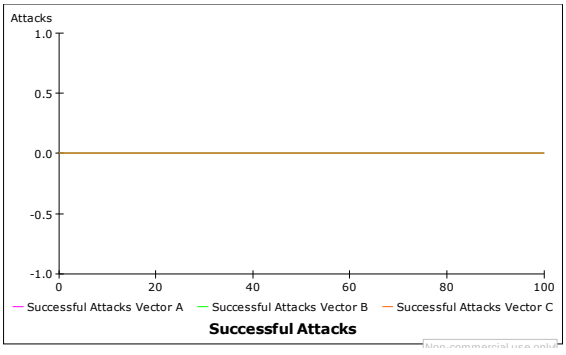


Figure 17 Equilibrium Run: Successful Attacks

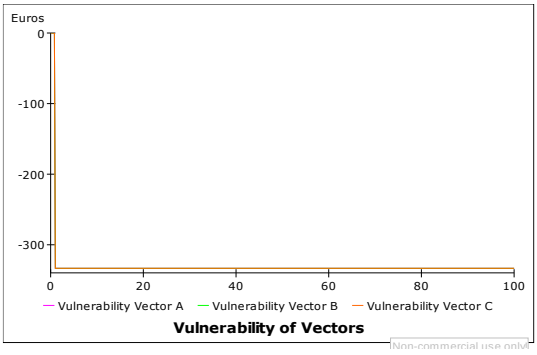


Figure 16 Equilibrium Run: Vulnerability of Vectors

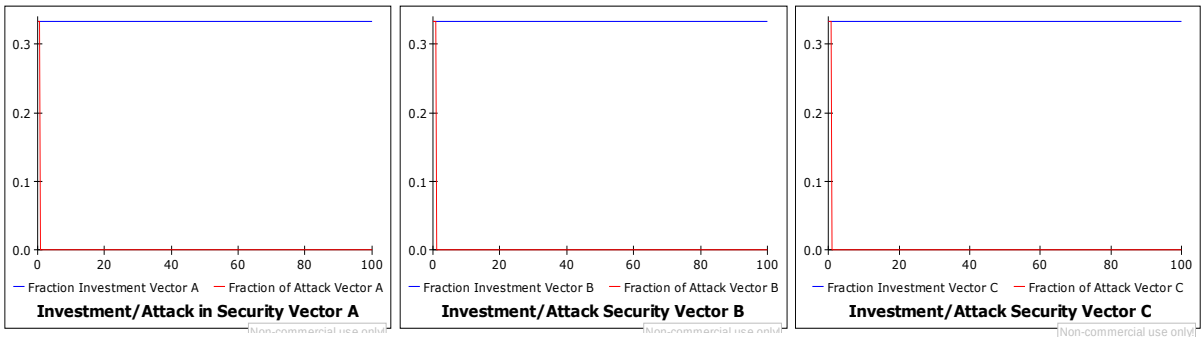


Figure 18 Equilibrium Run: Investment/Attack in Security Vectors

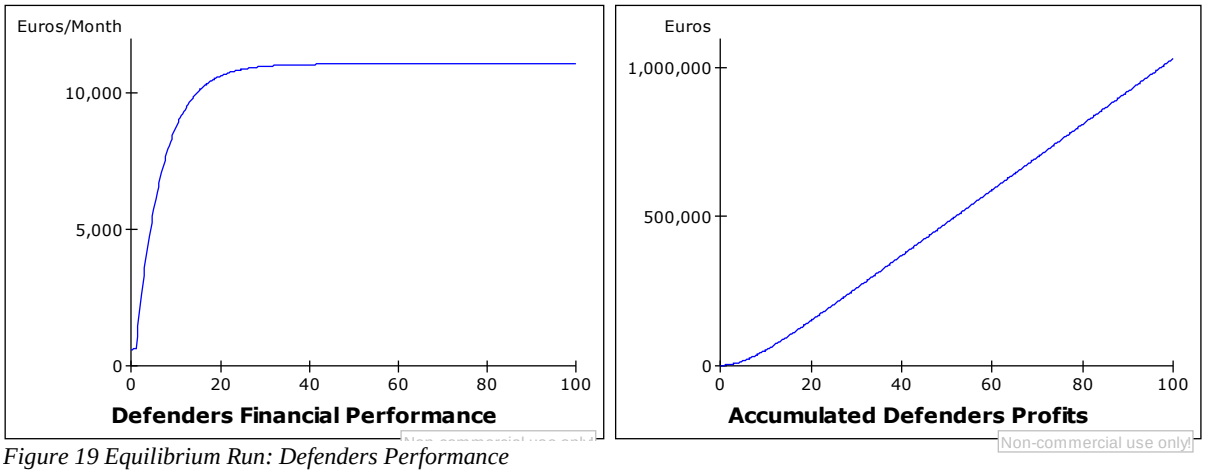


Figure 19 Equilibrium Run: Defenders Performance

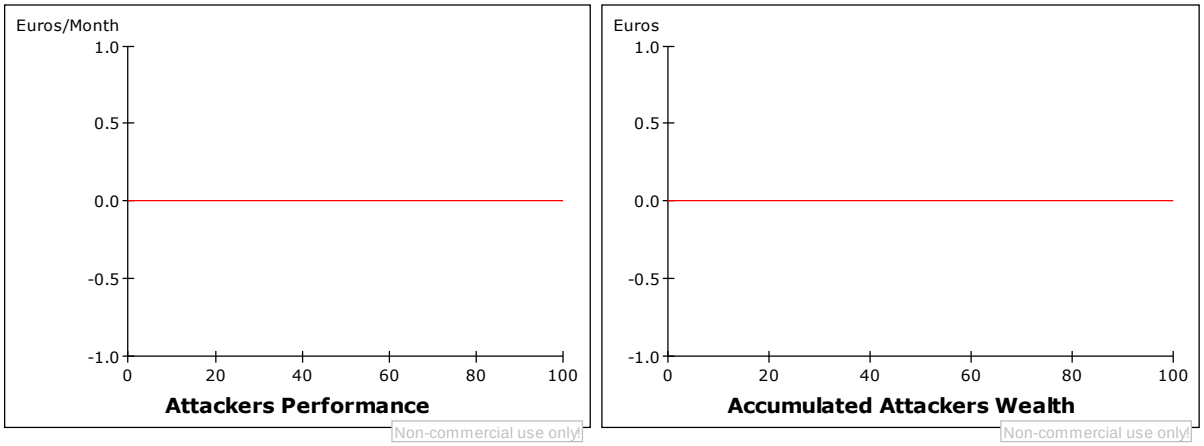


Figure 20 Equilibrium Run: Attackers Performance

Chapter 6: Model Validation

6.1 Model Validation Overview

Any audience for a model-based study want to know how much trust to place in analyses based upon the model. The system dynamics modeling process is iterative, in which various tests are used to scrutinize the model and to place confidence in its usefulness, such process generates insights into the relationships between system structure and behavior. The formal processes that lead people to place confidence in a model, are frequently referred to as the validation of the model (Richardson & Pugh, 1981). There is little agreement among different modeling methodologies about what a good validation is or should be. In fact, there is no general appropriate procedure for validation that a system dynamics model must go through to be considered as validated (Barlas, 1996; Sterman, 2000).

The iterative approach to the formulation of a model is usually forced by the complexity of the problem being addressed. However, despite numerous iterations in the modeling process, no model has ever been or ever will be thoroughly validated (Greenberger et al., 1976), mostly because they are all simplified representations of reality. Therefore, all models are wrong as stated by Sterman (2000).

Barlas and Erdem (1994), remark that validity in system dynamics refers to the internal structure of the model rather than the output behavior. Behavior replication alone is not sufficient to assume validity, as it is possible to obtain the "right behavior for the wrong reason". Instead, models have a certain purpose against which their validity can be tested, then the validation process should be directed to achieve the goal of the model.

Despite the limitations of validation restricting from its qualitative and iterative nature, Barlas (1996) proposed a logical sequence as a guideline for carrying out model validity tests in three stages: direct structural tests, structure-oriented tests, and behavior pattern prediction. Any of these tests by itself is certainly inadequate as an indicator of model validity. Taken together, they are a formidable filter, capable of trapping and weeding out weaker models and allowing those that are most likely to reflect something close to truth. The model in the present research follows this guideline. The procedures for conducting the tests are explained further together with descriptions of the respective tests.

6.2 Structure Validity

6.2.1 Direct Structure Tests

Direct structure tests assess the validity of the model structure, by direct comparison with knowledge about real system structure. This means comparing each equation and logical function individually of the model with the relationships available knowledge about the real system. In such tests, there is no simulation involved. The following tests belong to the category of theoretical structure test which involve comparing the model structure with generalized knowledge about the system that exists in the literature given the purpose of this model as mentioned in Chapter 1.

Structure-confirmation Test

The goal of this test is to compare the model equations with the relationships that exist in the real system (Forrester & Senge, 1980), in this case, the conceptual foundation of the model is grounded in the systematic literature review in information security during the model-building process. An example of structure-confirmation performed during the modeling process relates to the structure of how the security level of each security vectors and the potential loss from such security vector, affects the investment strategy of the future distribution of capabilities among the vectors of access in order to protect the firm's information asset.

As portrayed in Figure 21, the most common used strategy by the defender to allocate information security expenditures is the "Wait-And-See" approach. Due to the uncertainty associated with potential information security breaches, security managers may consider economically rational to take a wait-and-see attitude toward spending the available security capabilities until a breach occurs. Once an attack is successful in a security vector, such attacks are constantly reported by the defense to be able to base their next decision of fraction of investments that will be addressed to the vector that is being breached the most.

According to the real options literature (Gordon et al., 2003; Pindyck, 1991), waiting for key events to occur will often yield higher expected benefits from capital investments than acting as if the investment needs to be made now or never.

This literature shows that before one makes the investment, the net present value (NPV) of making an investment today, needs to be greater that the option value associated with deferring the decision until more information is available.[17]

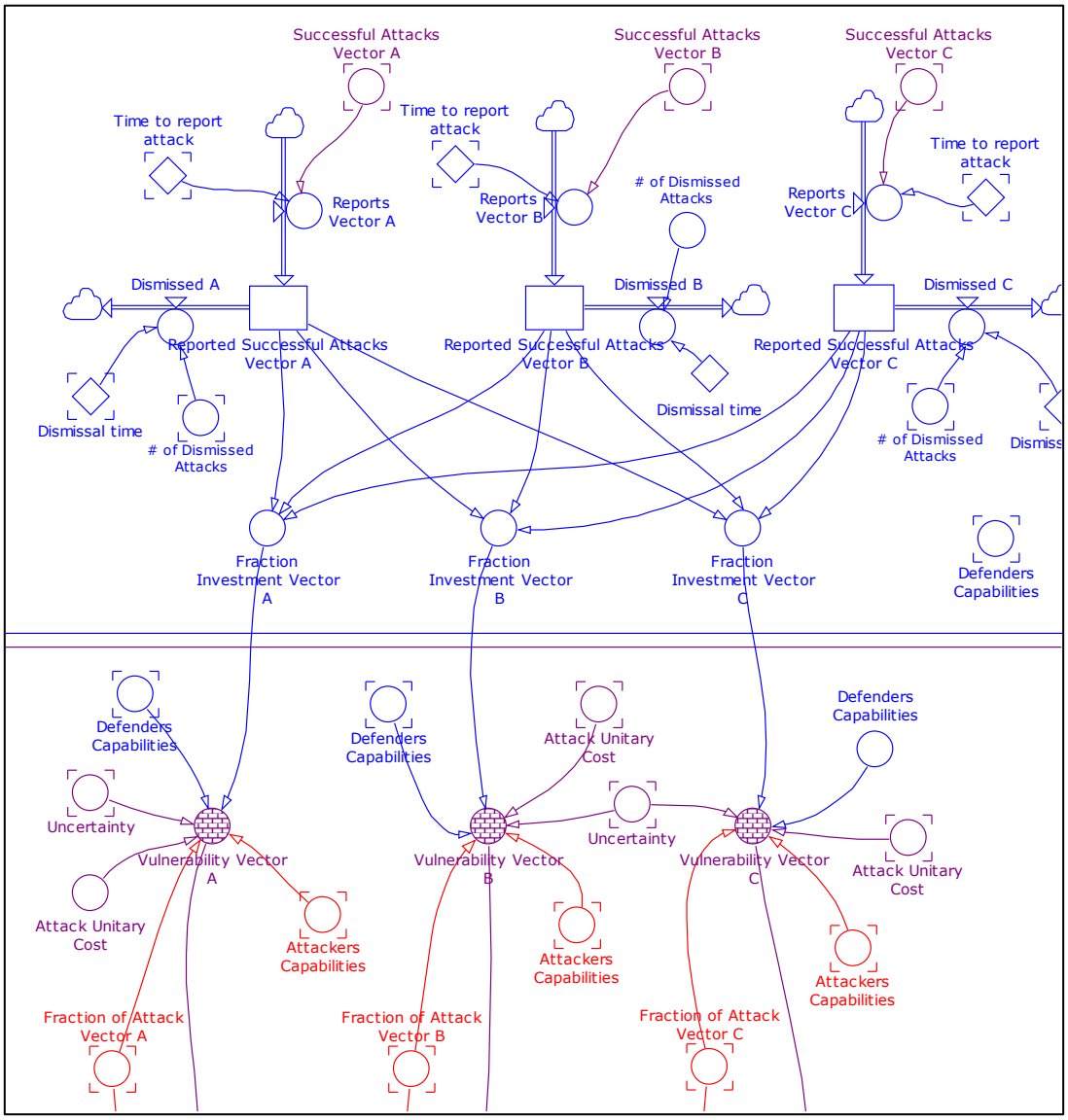


Figure 21 Structure-confirmation test: Wait-And-See Strategy

Parameter-confirmation Test

This assessment makes sure that the values of all parameters are reasonable and every variable and constant has a clear real-life meaning. The parameter confirmation was constantly evaluated against the knowledge available in the literature, both conceptually and numerically.

[7] See Gordon (2000, Chapter 12)

The conceptual confirmation was performed by identifying the elements available in the literature that correspond to the parameters of the model. The numerical confirmation was conducted by estimating the numerical value of the parameter with enough accuracy and plausible ranges.

Some technical parameters are created only for modeling purpose, while no real data is available. For instance, some technical parameters such as capabilities and attack unitary costs were estimated to illustrate the dynamics of defender and attacker investment strategies.

Attacks can originate from inside or outside of the firm. The model does not differentiate between internal or external attackers. Similarly, it does differentiate between attacks on different information assets which are beyond this research scope.

By examining the values for all the parameters in the model, it helps us to get a more accurate and reliable understanding of the model and we find out the aggregated structure is acceptable for the research purpose.

Direct extreme-condition Test

This test supports that each decision (model equations) result in plausible output under extreme values. The test was conducted by assessing the plausibility of the resulting values against the knowledge/anticipation of what would happen under a similar condition in the real system (Forrester & Senge). The output of this test can be deduced without needing simulation, it is applied by inspection of each equation in isolation.

For each flow in the model, the equations were put into extreme conditions, tracing back as well the stocks involved. For instance, imaginary max and min values were introduced to the input variables and compare the value of the output variable to what would logically happen in the real system under same extreme conditions.

To provide an example of this test, the flows Breaches for Attackers and Reported Attacks for Defenders were tested. These flows represent the attacks that were successful and driving attackers to identify and exploit the weakest link and defenders to also identify the weakest link and defend their asset.

The flows are formulated by the following equations:

Breaches Vector *i* = Successful Attacks/Time to report attack

Reports Vector *i* = Successful Attacks/Time to report attack

Assuming that Defenders Capabilities drastically increase surpassing the Attackers Capabilities, there will be therefore no successful attacks and the defender will be benefited. Meanwhile, if the Attackers Capabilities increases radically outweighing the Defenders Capabilities, the successful attacks will increase dramatically harming the Defenders and favoring the Attackers.

Dimensional Consistency Test

A system dynamics model has dimension for each of its variables. The dimension for each variable is specified when the model is built, the dimensional consistency test reflects nothing more that unit error or missing units. The dimensional consistency test has been performed automatically by the system dynamics software employed for this research (Powersim Studio 9), which does not allow the model to run without all equations being dimensionally consistent. This test helps assessing whether the units match on the left and right hand side of each equation without using any arbitrary "scaling" parameters that have no real world meaning (Barlas, 1996; Sterman; 2000). This model is considered dimensionally consistent since it generates no unit error messages when running the simulations.

6.2.2 Structure-Oriented Behavior Tests

This set of tests assess the validity of the structure indirectly by applying certain behavior test on model-generated behavior patterns (Barlas 1989, Forrester & Senge, 1980). These tests involve simulation and are considered strong behavior tests that can help the modeler to uncover potential structural flaws.

Extreme-Condition Test

This test implicates assigning extreme values to certain parameters and comparing the model-generated behavior of the observed or anticipated behavior of the real system under the same condition.

A good example for the extreme-condition test is the Defenders and Attackers Capabilities. These parameters are exogenous in the model and play an important role in determining the security level of each vector of access to the information asset that the firm is trying to protect.

For instance, higher capabilities for either of the two adversaries will mean and increase or a decrease in the security level of each vector, which therefore will be translated into more or less-successful attacks triggering investment strategies for future periods.

An extreme-condition test involving Defenders Capabilities can help test whether the descried mechanism follows a robust formulation. This is particularly important since if firms dedicate a higher budget to security measures, it would mean more protection and fewer successful breaches into the firm's asset. However, a sudden change in this parameter is not realistic because companies often have a relatively fixed budget for security actions. On the other hand, Attackers Capabilities might experience a drastic drop or boost in life, however, cyber criminals are IT professionals that are methodic in their operations. This means that they have certain level of capabilities they can plan on to run their business model.

Figure 22, shows the model's response to extreme-conditions for Defenders Capabilities. As the figure shows, the Defenders capabilities where changed to 10,000 Euros, meanwhile the Attackers Capabilities remained the same. Since the defenders can protect more their asset in all their vectors, their financial performance increase since they maintain their reputation high and the attackers are not able to breach any of the vectors and their wealth is zero.

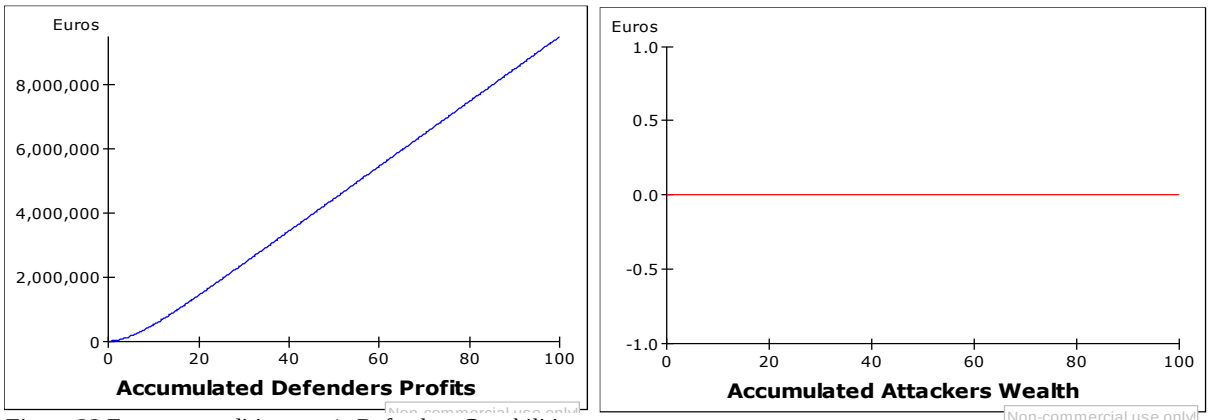


Figure 22 Extreme-condition test 1: Defenders Capabilities

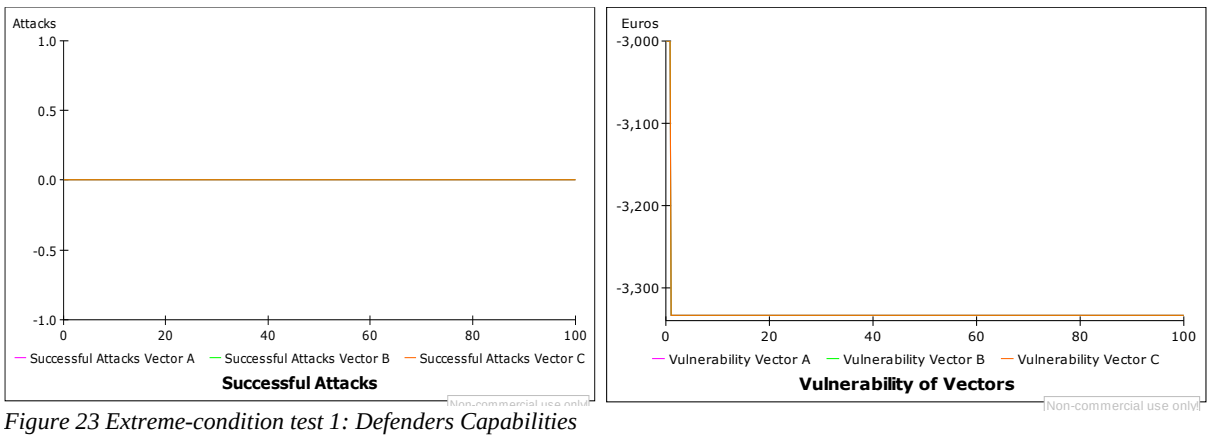


Figure 23 Extreme-condition test 1: Defenders Capabilities

Figure 24 and 25, shows the model's response to extreme-conditions for Attackers Capabilities. As the figure illustrates, the attacker's capabilities where changed to 1,000 Attacks, meanwhile the defenders' capabilities remained the same. Since the defenders cannot protect their asset in neither of their vectors, their financial performance drops drastically as their reputation is very low, so the attackers can breach all the defender's vectors and their wealth increases.

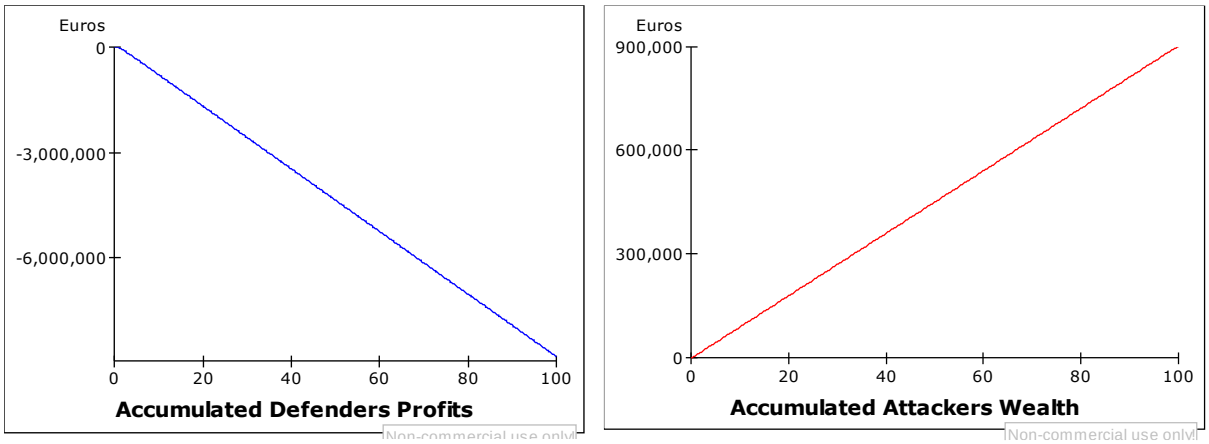


Figure 24 Extreme-condition test 2: Attackers Capabilities

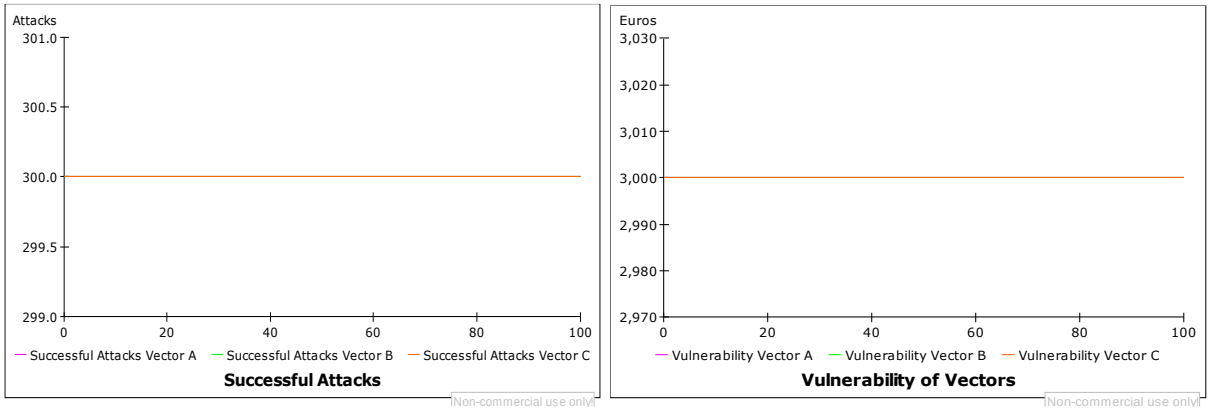


Figure 25 Extreme-condition test 2: Attackers Capabilities

Behavior Sensitivity Test

Behavior sensitivity test consists of determining those parameters to which the model is highly sensitive and asking if the real system would exhibit similar high sensitivity to the corresponding parameters. The following simulations represent the sensitivity analysis performed first, in the model's initial conditions for the accumulated successful attacks of the attackers for vectors A, B and C. Then, sensitivity analysis was conducted with changes in unitary cost of attack (damage).

Initial conditions of the stocks for Attackers

Vector A=5 Vector B=5 Vector C=10

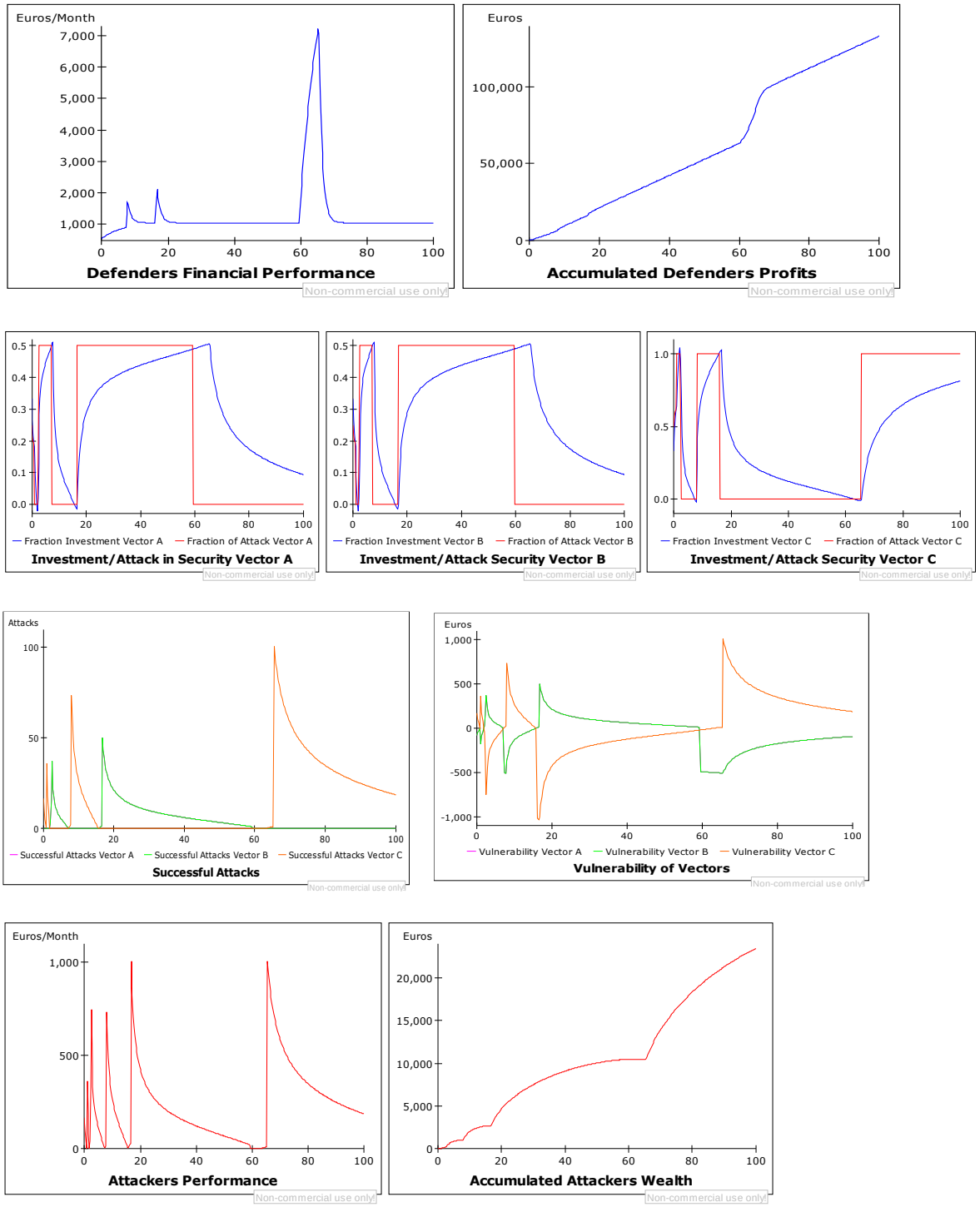


Figure 26 Sensitivity test 1

Initial conditions of the stocks for Attackers

Vector A=10 Vector B=10 Vector C=5

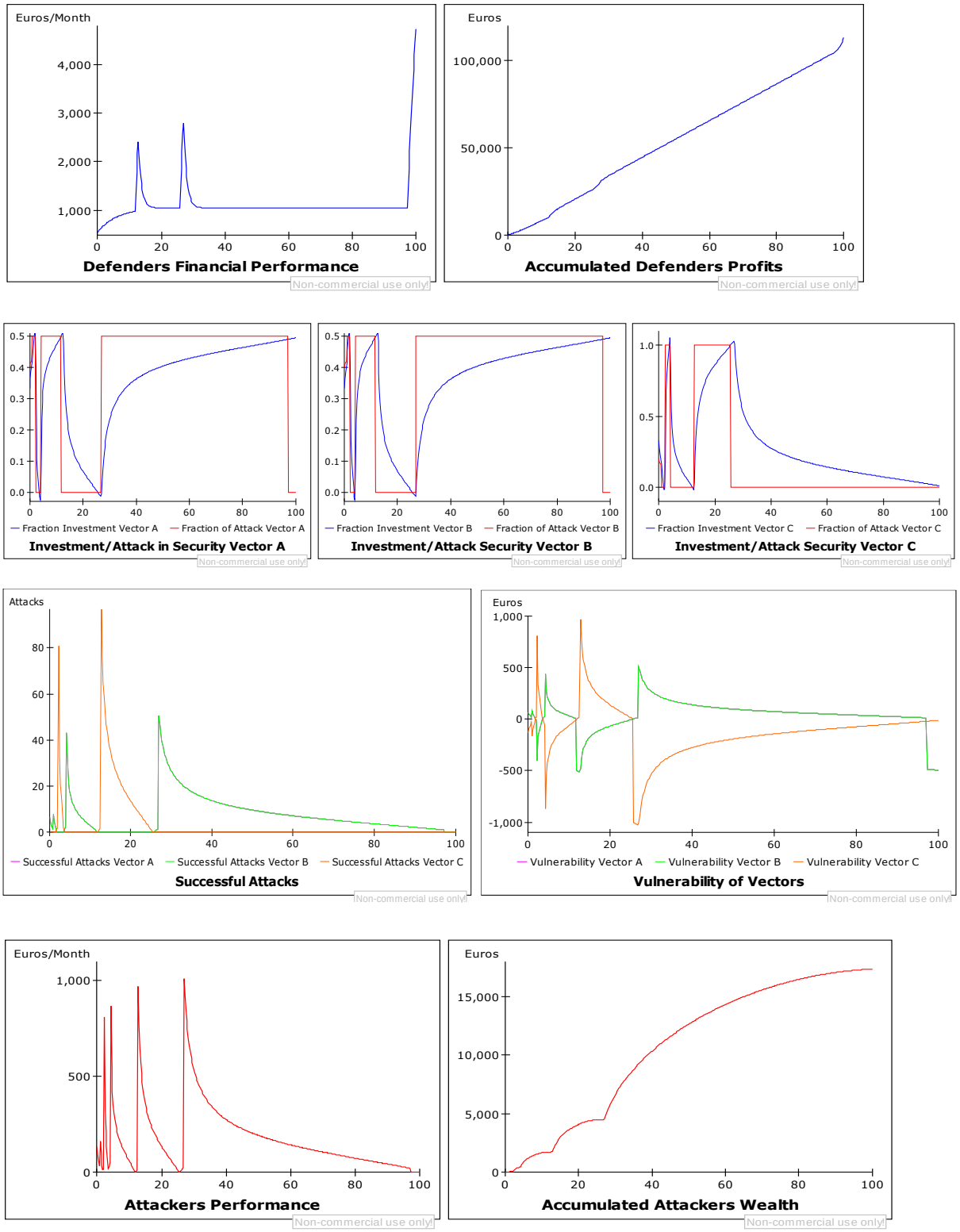


Figure 27 Sensitivity test 2

Initial conditions of the stocks for Attackers

Vector A=5 Vector B=10 Vector C=5

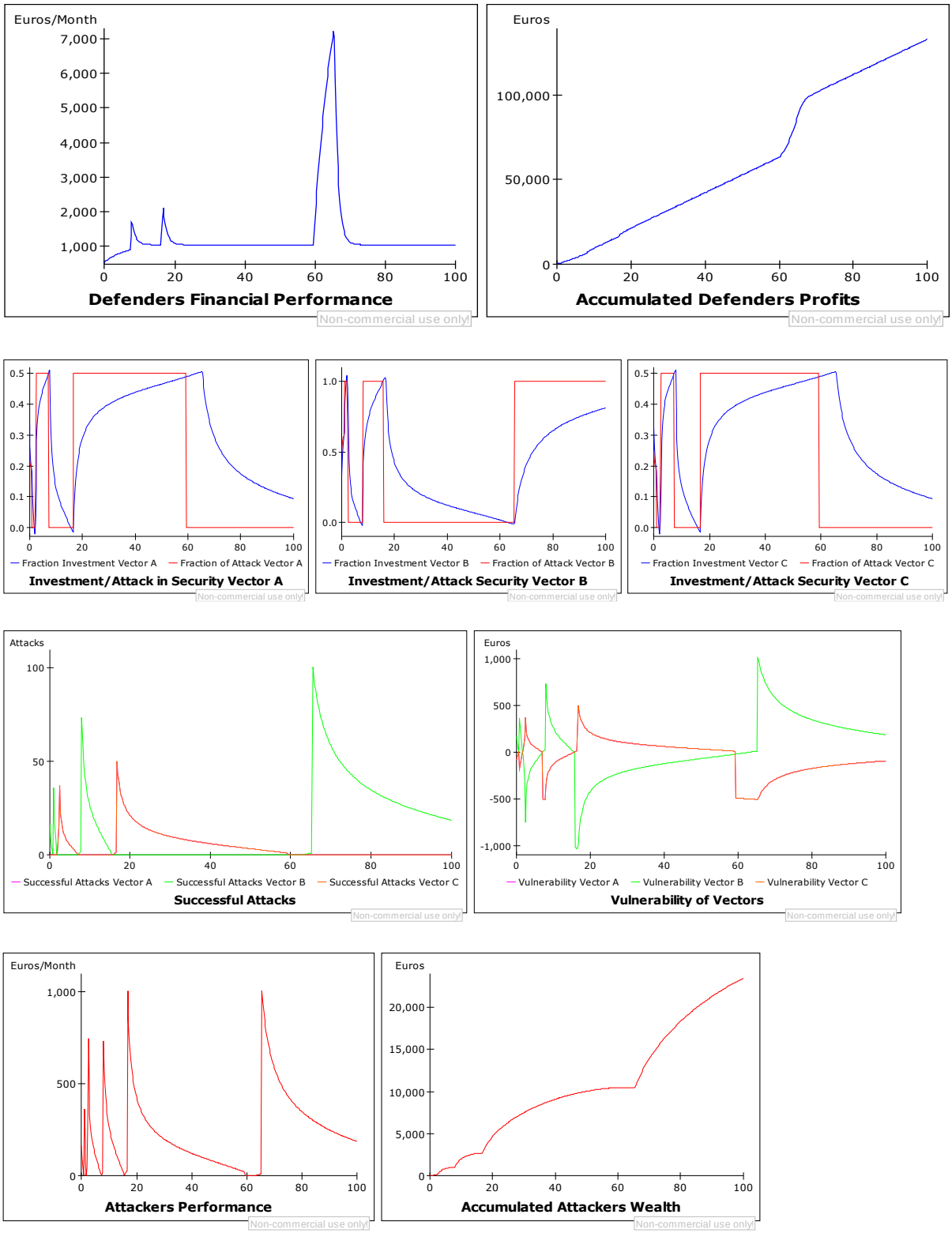


Figure 28 Sensitivity test 3

Attack Unitary Cost

Attack Unitary Cost= 5

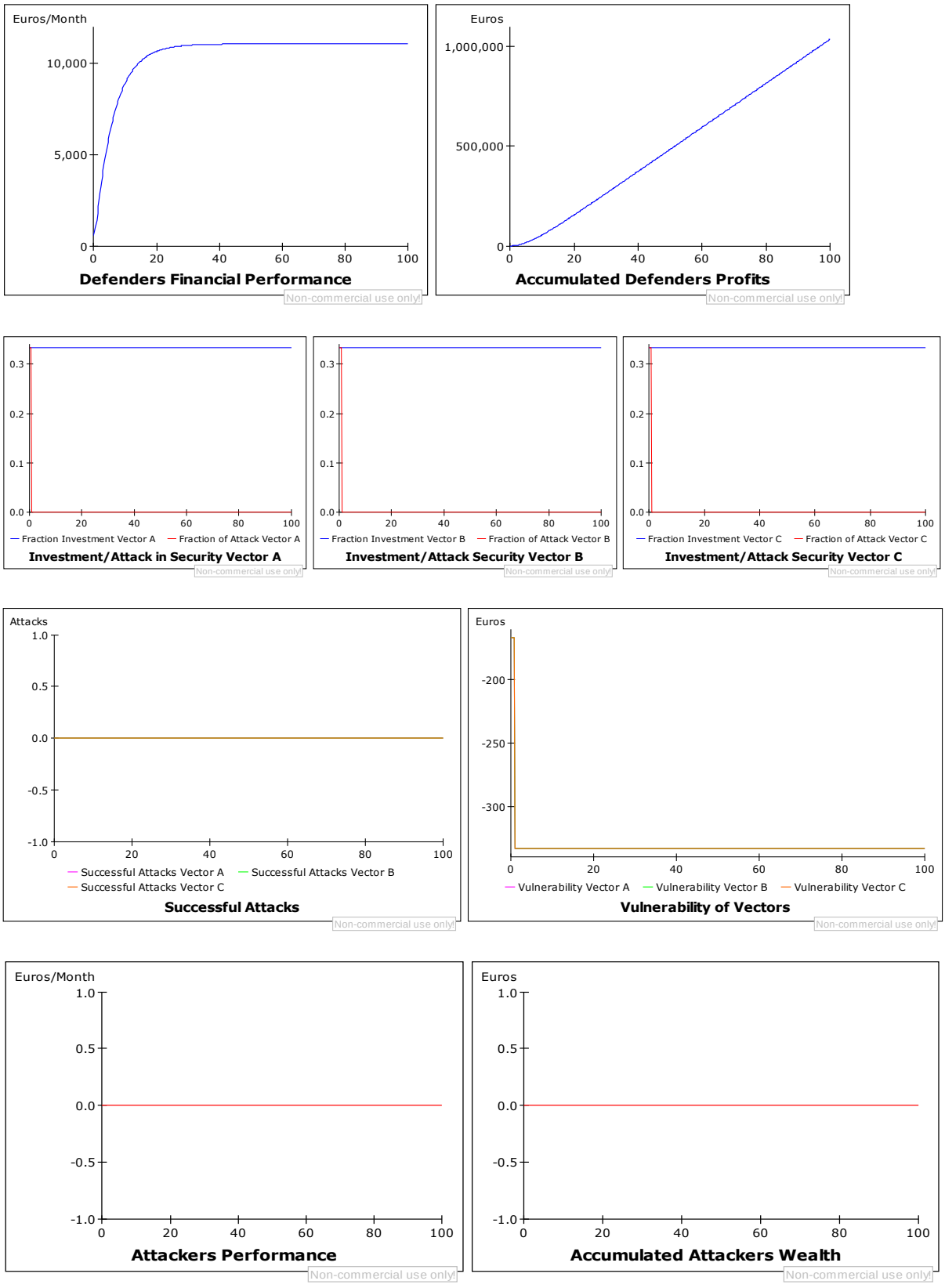


Figure 29 Sensitivity test 4

Attack Unitary Cost= 15

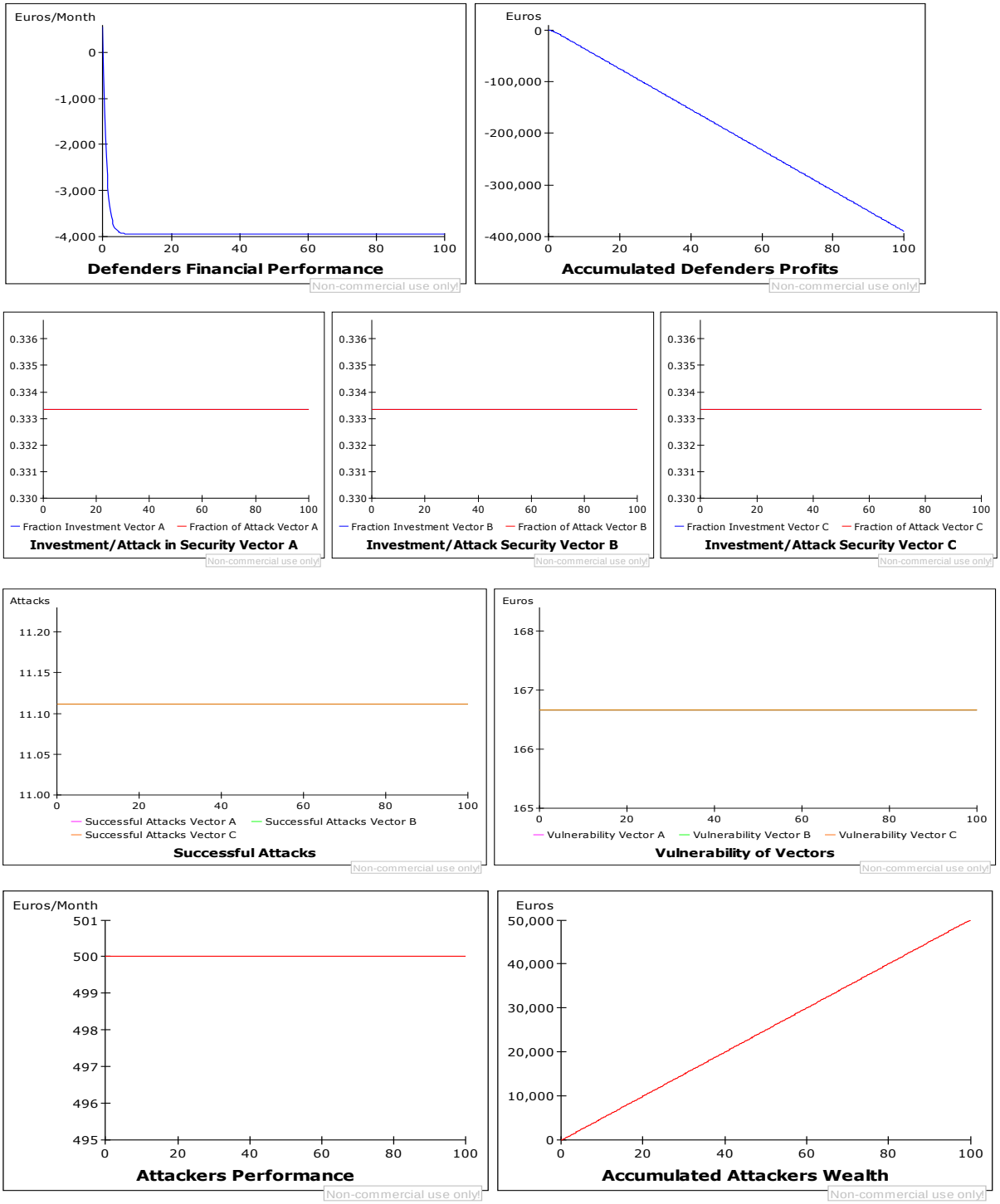


Figure 30 Sensitivity test 5

The results of the sensitivity test showed that the model is highly sensitive initial conditions for the accumulated successful attacks of the attackers for vectors A, B and C; and unitary cost of attack (damage). The results are consistent with the behavior of the real system according to the existing knowledge available in the literature.

Integration method and DT Error Tests

System Dynamics models are usually formulated in continuous time and solved by numerical integration. The integration method selected to construct this model was 4th order, Runge-Kutta (fixed step) with time step equal to 0.25, meaning that since the simulation is run in months, the time step will display attacks happening weekly. These choices were made this way in order to yield an approximation of the underlying continues dynamics that are accurate enough according to the purpose of the model.

The integration method test consists in alternating the current integration method to another, in this case, the model was changed to run with 1st order, Euler (fixed step) integration method. As a note, this test was the first simulation test carried out to avoid failures in the model results. This test revealed that there are not significant differences in the behavior or the model.

The DT error test aims to find out whether the model is sensitive to the settings of time steps. This test is conducted by cutting the time step in half from 0.25 to 0.125 and running the model again. The result of this test was that the model is not sensitive to changes in DT.

6.3 Behavior Validity

Behavior Pattern Tests

Once enough confidence has been built in the validity of the model structure, the behavior pattern tests are usually conducted to measure how accurately the model can reproduce the major behavior patterns exhibited by the real system. Generally, this test involves comparing the generated behavior of the model with the reference mode (behavior of the real system). However, the reference model of this study does not have available data. Instead, the nature of the problem created the context that we are modeling based on the concepts existing in the literature regarding information security.

To conclude this chapter, the validation of the model relies primarily on the structure and structure-oriented behavior tests. The behavior pattern testing can be conducted only based on the available knowledge in the information security literature. Nevertheless, this model demonstrated the historical reference mode of the problem undertaken in this study, which was justified by the nature of the problem and its purpose.

Chapter 7: Scenario Analysis

The purpose of this chapter is to answer the fourth research questions by testing the hypothesis that the Wait-and-see and Weakest Link approaches are no longer effective strategies when making investment decisions under uncertainty.

7.1 Scenario Description

The conditions for each scenario were considered based on the base run, information asymmetries in defender/attacker capabilities and in security vector values. These three conditions were selected due to:

- First, the base scenario shows the behavior of the system when capabilities and vector values are equal. This allows the WL and WAS strategies to operate both with and without uncertainty.
- Second, defenders and attackers' capabilities determine how likely the attackers are to exploit the vectors with the WL strategy, and how likely the defenders are to react to breaches based on the WAS strategy. If the attacker has higher resources than the defender, he will be able to breach the defenses in vectors. On the other hand, higher defenders' capabilities mean that the defenders will be able to block all incoming attacks, which means no reaction to breaches (since they never come to be) and thus, no use of the WAS strategy.
- Finally, asymmetries in vector value yield more realism to the analysis, since in reality, security vectors have different weight in values. Therefore, when breaches happen in a valuable vector, this can cause a greater or lower damage in performance of the defender depending on such vector's value.

The scenario space is a matrix of outcomes for alternative conditions against anticipated scenarios, such matrix constructed for this section consists of a 3 by 4 matrix composed by: base scenario conditions, asymmetric capabilities and asymmetric vector values against a base scenario with uncertainty equal to zero and three levels of uncertainty classified in low, medium and high uncertainty.

Scenarios illustrate what is the effect of a change in capabilities from both parties and in the weight of value that each security vector, in financial performance of defenders and attackers and in successful attacks under different levels of uncertainty. Figure, shows the portion of the model concerning uncertainty levels.

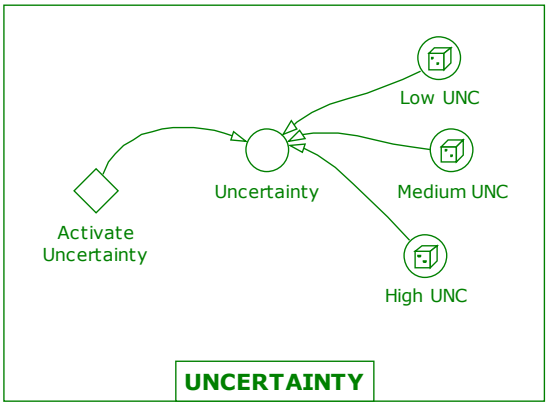


Figure 32 Scenario Analysis: Uncertainty levels

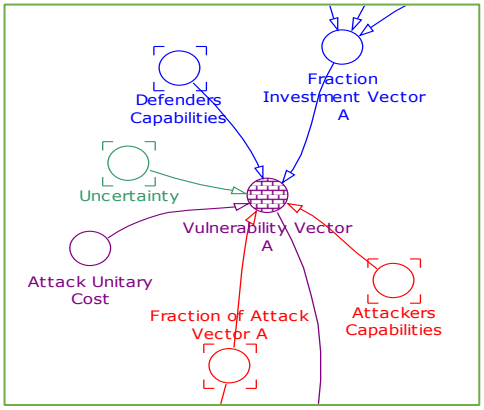


Figure 31 Scenario Analysis: Uncertainty

When activated, uncertainty is a multiplier of the attack unitary cost that determines each security vector's vulnerability, as shown in Figure. A continuous uniform distribution[8],also known as rectangular distribution was chosen to perform the scenario space analysis.

Given that this study is a theoretical framework of the cybersecurity field, the scenarios were analyzed given a constant probability of having higher or lower damages of cyber-attacks by assuming a minimum and maximum value in each uncertainty level. A uniform distribution is given by the formula:

$$\mathbf{f(x) = (\mathit{Max} - \mathit{Min})^{-1}, \text{ when } \mathit{Min} < x < \mathit{Max}}$$

Disproportional ranges of uncertainty were selected as Low= U(0.95, 1.1), Medium= U(0.875, 1.25) and High= U(0.75, 1.5); to allow more dynamic investment strategies between defenders and attackers. If we assume a balance distribution around 1, the defender will likely shut down all the successful attack opportunities for the attacker. To avoid this, we restrict the lower boundary of the uniform distribution that benefits the defender hinders the attackers such that the distance from the lower boundary to 1 is half of the distance between 1 and the upper boundary. Each range of uncertainty is calculated with a RANDOM function which generates a series of random numbers that are distributed according to the uniform distribution.

[8] In a uniform distribution, all intervals of the same length on the distribution's support are equally probable. The support is defined by the two parameters, a and b, which are its minimum and maximum values (Cassela & Berger, 2001). The distribution is often abbreviated U(a,b).

Scenarios with uncertainty were simulated with the risk analysis component in Powersim Studio Software version 9. The sampling technique used for sensitivity simulations was Latin Hypercube Sampling technique[9], running the model 100 times to obtain an average simulation in the final run, since a uniform distribution is being used.

The scenario space analysis is presented with an outline of scenarios followed by three parts:

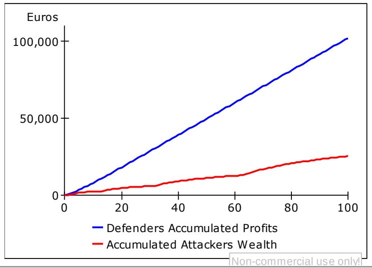
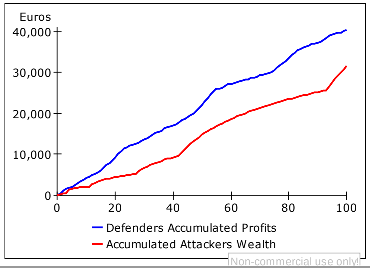
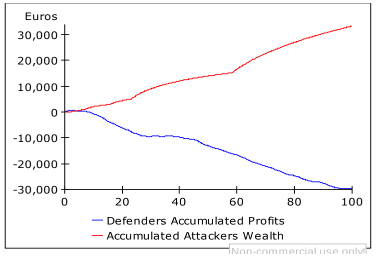
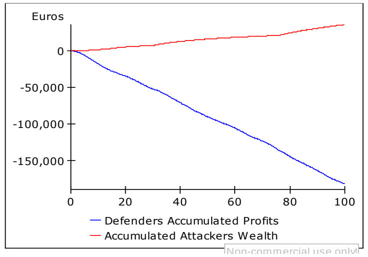
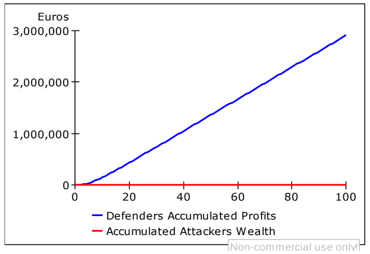
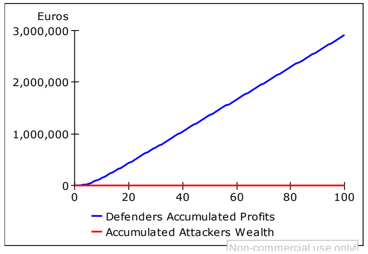
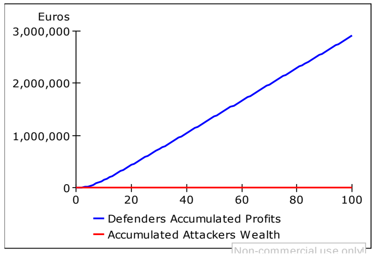
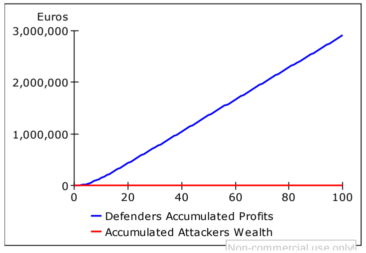
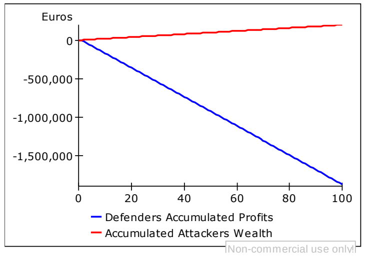
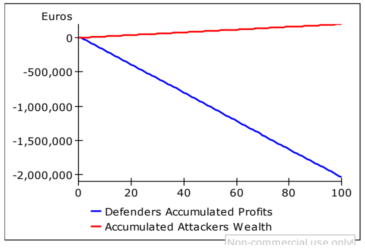
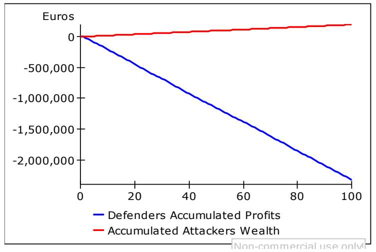
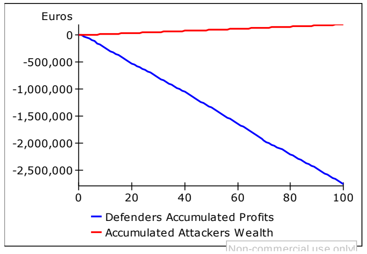
- The first diagram, Scenario Model Behavior: Changing the parameters, shows how the parameters were changed to operationalize the scenarios of each cell.
- The second diagram, Scenario Model Behavior: Defender/Attacker Performance, shows how one key indicator changes with respect to each change in the level of uncertainty affecting the financial performance of the adversaries.
- The final chart Scenario Model Behavior: Successful Attacks, illustrates how changes in key indicators influence the successful attacks on each security vector.

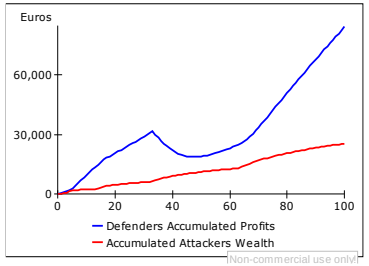
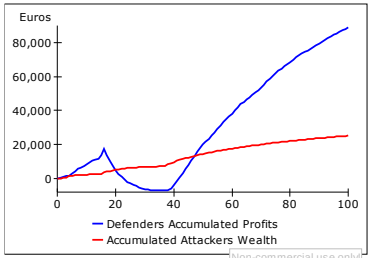
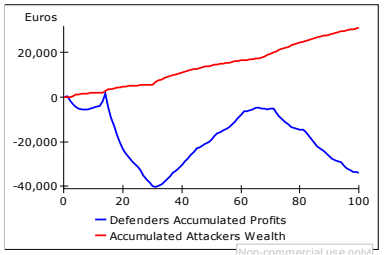
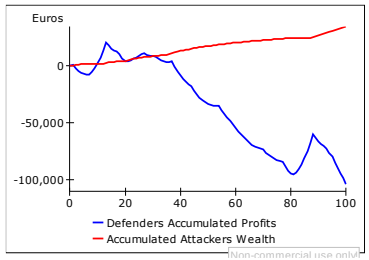
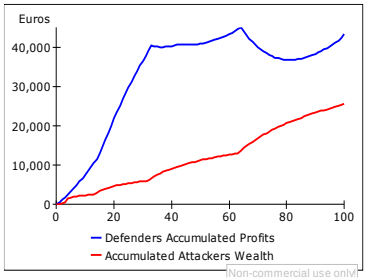
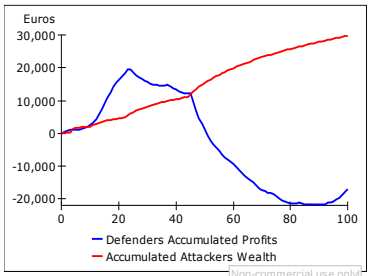
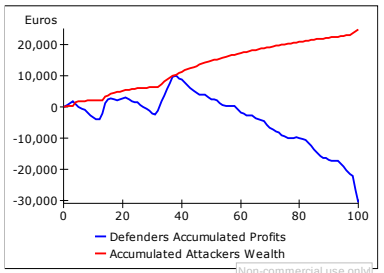
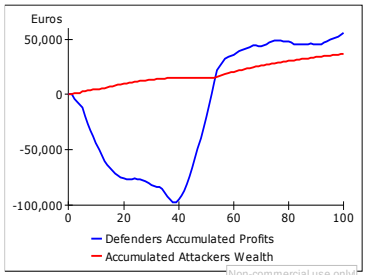
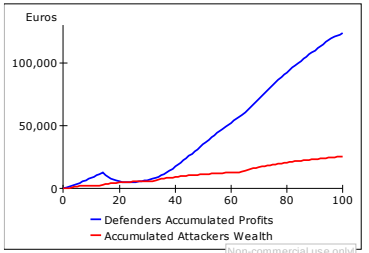
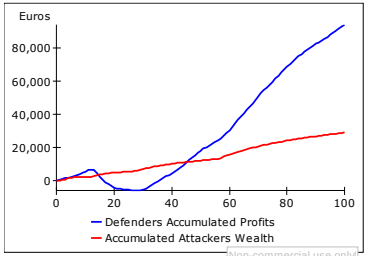
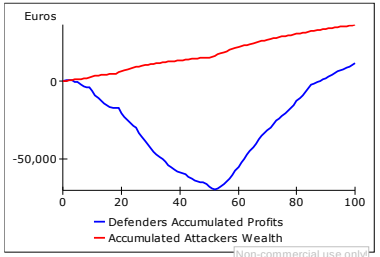
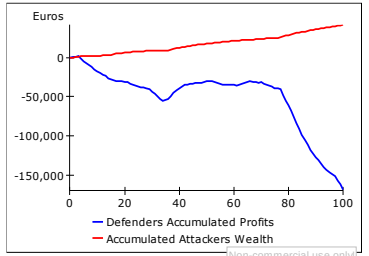
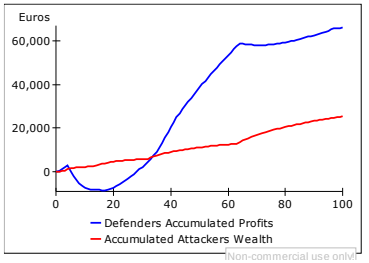
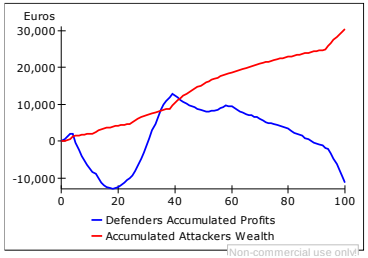
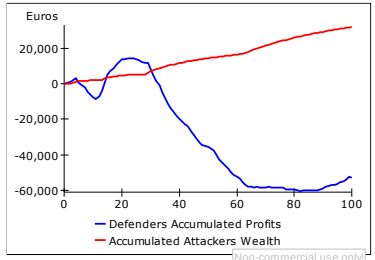
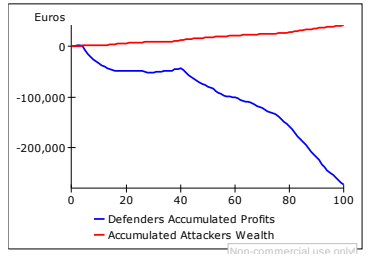
[9] The Latin Hypercube Sampling (LHS) technique is the recommended sampling method. Formal comparisons have revealed that LHS is a highly efficient way to test a model (Ford, 2010) It combines the advantages of simple random sampling (as used in the Monte Carlo technique), and full factorial designs. This means that all areas of the sample space are represented. The probability distribution of each assumption is segmented into several non-overlapping intervals with equal probability (McKay et al., 1979).

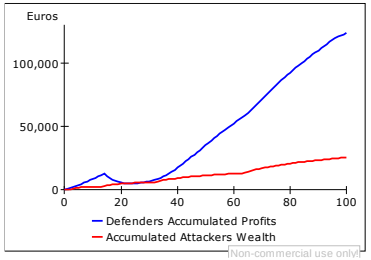
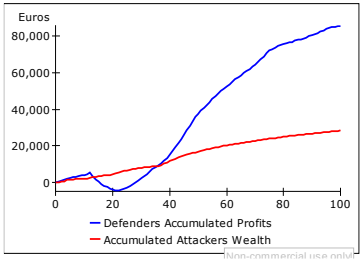
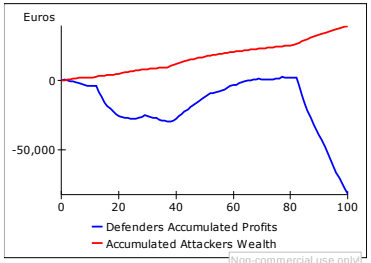
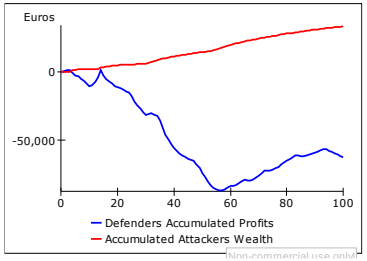
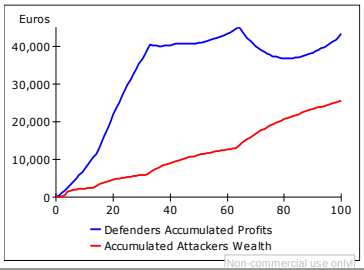
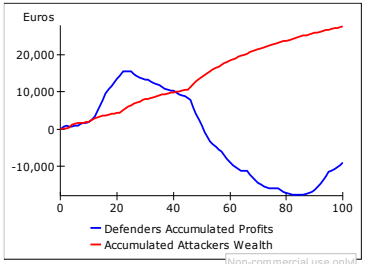
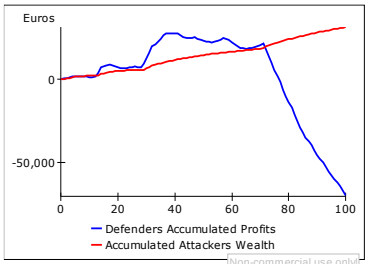
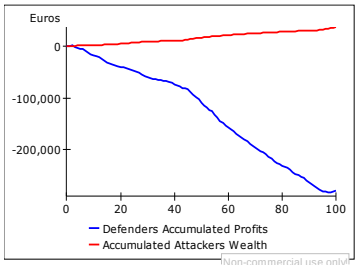
7.1.1 Scenario Model Behavior: Changing the Parameters

	No Uncertainty	Low Uncertainty	Medium Uncertainty	High Uncertainty
Scenario #1 Base Scenario	▪ Uncertainty = 1 ▪ Base run initial conditions ▪ Defense Capabilities = Attackers Capabilities ▪ Attack Unitary Cost = 10 ▪ Equal Vector Values (A, B and C = 1)	▪ Base run initial conditions ▪ Defense Capabilities= Attackers Capabilities ▪ Attack Unitary Cost= 10 * U (0.95,1.1) ▪ Equal Vector Values (A, B and C = 1)	▪ Base run initial conditions ▪ Defense Capabilities= Attackers Capabilities ▪ Attack Unitary Cost= 10 * U (0.875,1.25) ▪ Equal Vector Values (A, B and C = 1)	▪ Base run initial conditions ▪ Defense Capabilities= Attackers Capabilities ▪ Attack Unitary Cost= 10* U (0.75,1.5) ▪ Equal Vector Values (A, B and C = 1)
Scenario #2 Asymmetric Capabilities	▪ Uncertainty = 1 ▪ Defense Capabilities> Attackers Capabilities ▪ Attackers Capabilities> Defense Capabilities ▪ Attack Unitary Cost= 10 ▪ Equal Vector Values (A, B and C = 1)	▪ Defense Capabilities> Attackers Capabilities ▪ Attackers Capabilities> Defense Capabilities ▪ Attack Unitary Cost= 10 * U (0.95,1.1) ▪ Equal Vector Values (A, B and C = 1)	▪ Defense Capabilities> Attackers Capabilities ▪ Attackers Capabilities> Defense Capabilities ▪ Attack Unitary Cost= 10* U (0.875,1.25) ▪ Equal Vector Values (A, B and C = 1)	▪ Defense Capabilities> Attackers Capabilities ▪ Attackers Capabilities> Defense Capabilities ▪ Attack Unitary Cost= 10* U (0.75,1.5) ▪ Equal Vector Values (A, B and C = 1)
Scenario #3 Asymmetric Vector Values	▪ Uncertainty = 1 ▪ Defense Capabilities= Attackers Capabilities ▪ Attack Unitary Cost= 10 ▪ Vector Values: Max = 1.25 Medium = 1 Min = 0.75	▪ Defense Capabilities= Attackers Capabilities ▪ Attack Unitary Cost= 10 * U (0.95,1.1) ▪ Vector Values: Max = 1.25 Medium = 1 Min = 0.75	▪ Defense Capabilities= Attackers Capabilities ▪ Attack Unitary Cost= 10* U (0.875,1.25) ▪ Vector Values: Max = 1.25 Medium = 1 Min = 0.75	▪ Defense Capabilities= Attackers Capabilities ▪ Attack Unitary Cost= 10* U (0.75,1.5) ▪ Vector Values: Max = 1.25 Medium = 1 Min = 0.75

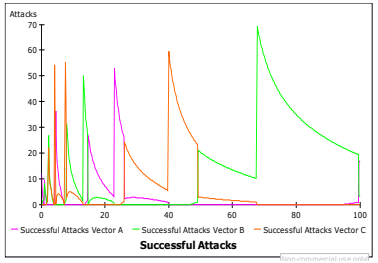
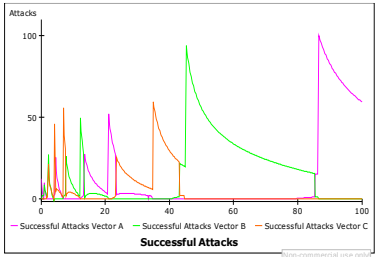
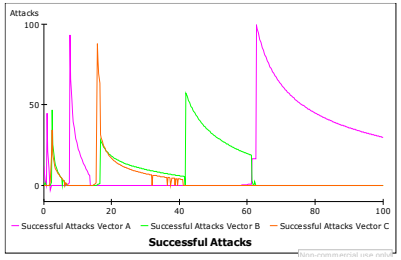
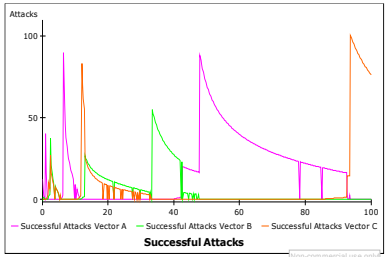
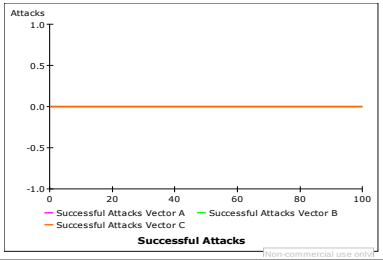
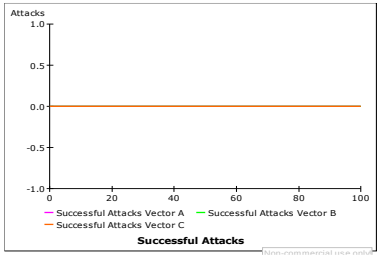
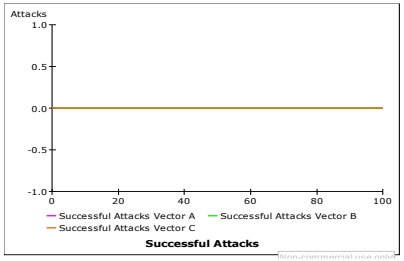
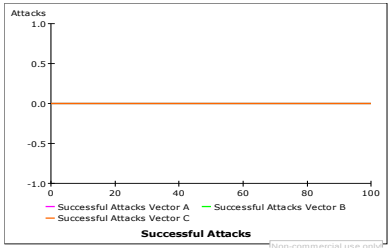
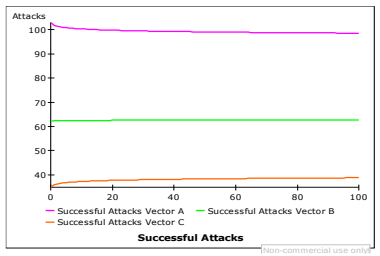
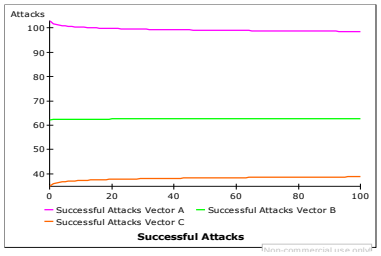
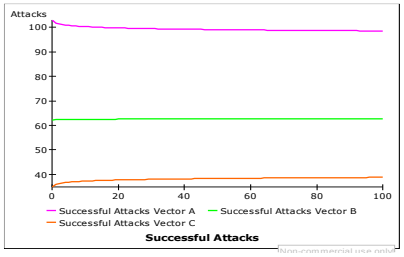
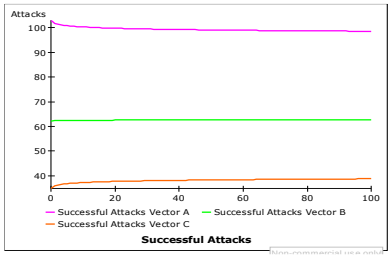
7.1.2 Scenario Model Behavior: Defender/Attacker Performance

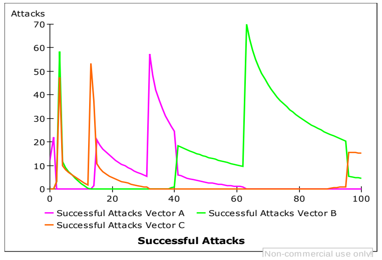
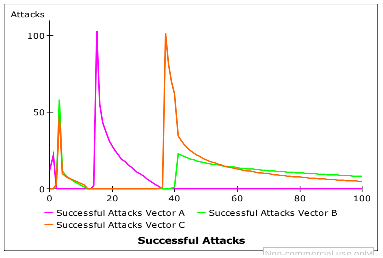
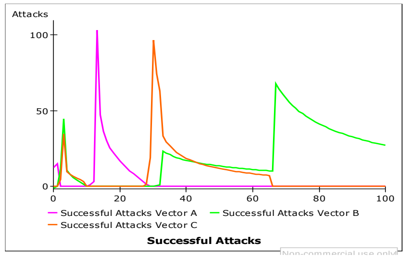
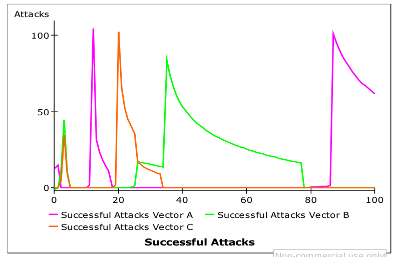
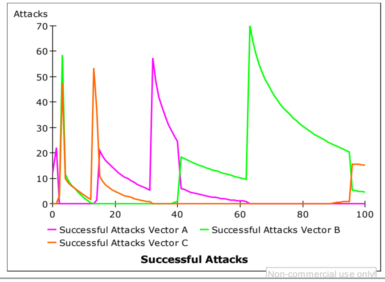
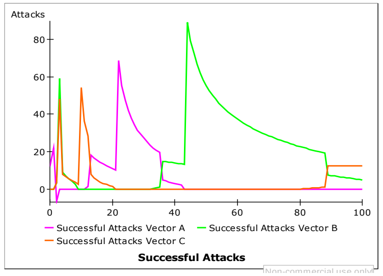
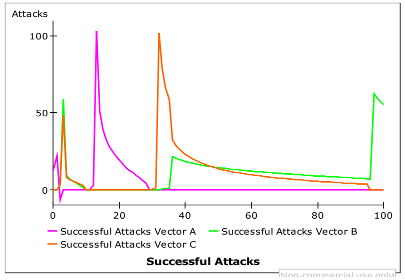
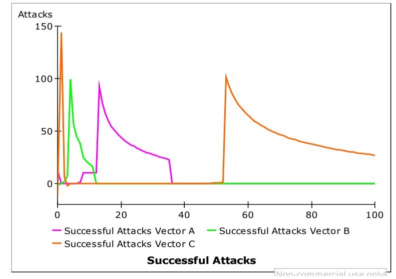
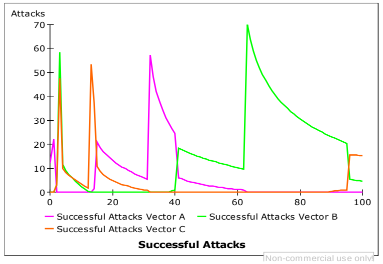
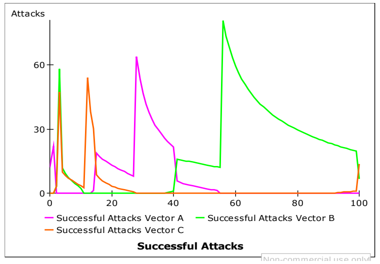
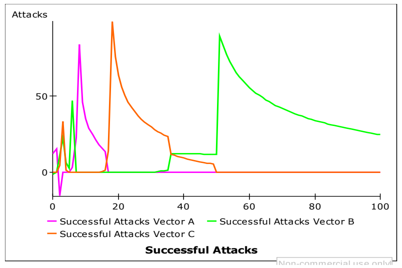
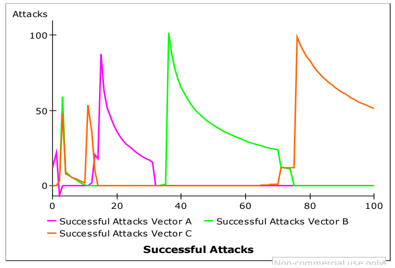
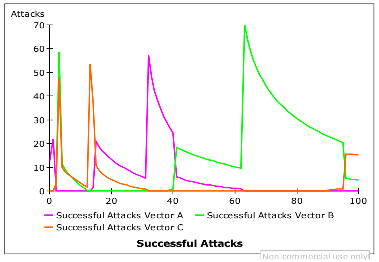
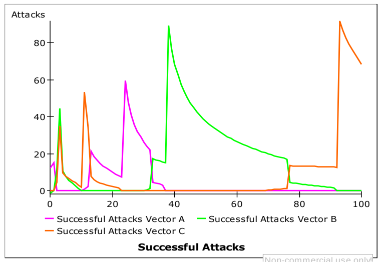
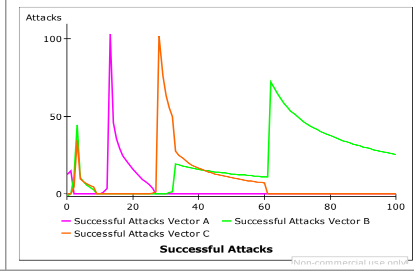
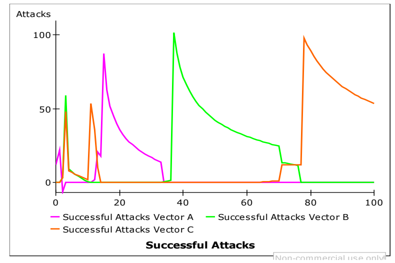
	No Uncertainty	Low Uncertainty	Medium Uncertainty	High Uncertainty
Scenario #1 **Base Scenario**				
Scenario #2 **Capabilities** **Defense = 3000** **Attacker = 100**				
Scenario #2 **Capabilities** **Defense = 1000** **Attacker = 300**				

Scenario #3 Vector Values A>B>C				
Scenario #3 Vector Values B>A>C				
Scenario #3 Vector Values C>A>B				
Scenario #3 Vector Values A<B<C				

Scenario #3 Vector Values B<A<C				
Scenario #3 Vector Values C<A<B				

7.1.3 Scenario Model Behavior: Successful Attacks

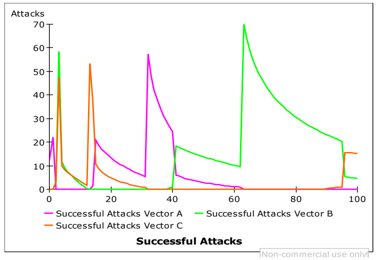
	No Uncertainty	Low Uncertainty	Medium Uncertainty	High Uncertainty
Scenario #1 Base Scenario				
Scenario #2 Capabilities Defense = 3000 Attacker = 100				
Scenario #2 Capabilities Defense = 1000 Attacker = 300				

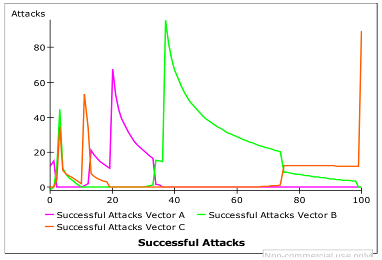
<table>
<tr>
<td>Scenario #3
Vector Value
A>B>C</td>
<td>  </td>
<td>  </td>
<td>  </td>
<td>  </td>
</tr>
<tr>
<td>Scenario #3
Vector Value
B>A>C</td>
<td>  </td>
<td>  </td>
<td>  </td>
<td>  </td>
</tr>
<tr>
<td>Scenario #3
Vector Value
C>A>B</td>
<td>  </td>
<td>  </td>
<td>  </td>
<td>  </td>
</tr>
<tr>
<td>Scenario #3
Vector Value
A<B<C</td>
<td>  </td>
<td>  </td>
<td>  </td>
<td>  </td>
</tr>
</table>

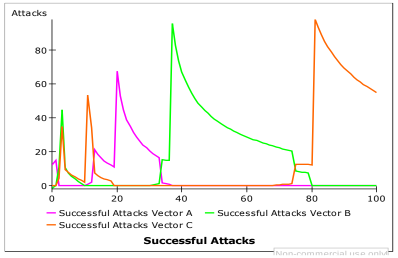
Scenario #3

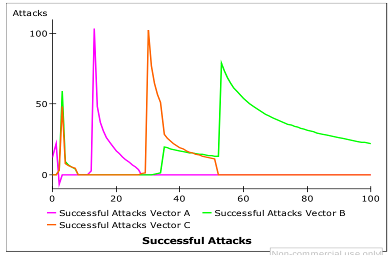
Vector Value

B<A<C





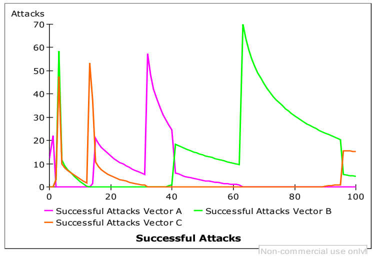


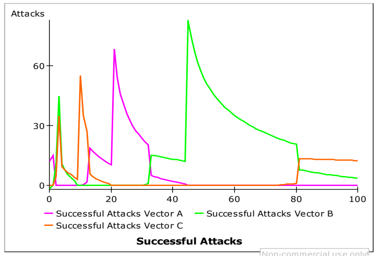


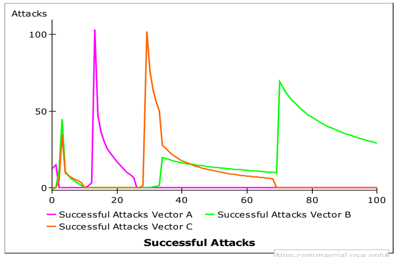
Scenario #3

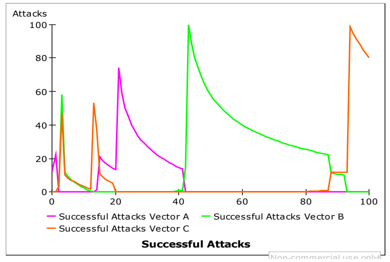
Vector Value

C<A<B









7.2 Description of Results of Scenario Analysis

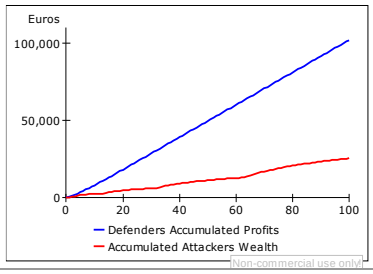
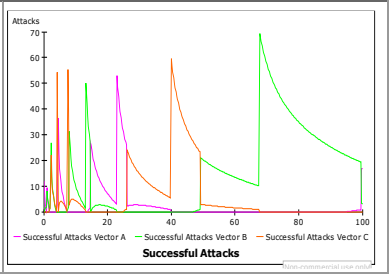
7.2.1 Scenario #1: Base Scenario

The base scenario describes the initial conditions already mentioned in the base run in Chapter. As the weakest link approach is operating in all scenarios, attackers have historical successful attacks (A=10, B=7 and C=5). Therefore, attackers are addressing all subsequent attack efforts in correspondence to these initial conditions. The following are the assumptions applied in the Base Scenario:

- Defenders and Attackers capabilities are the equal.
- Security Vector Values are the same. Vectors A, B and C are equal to 1.

No Uncertainty

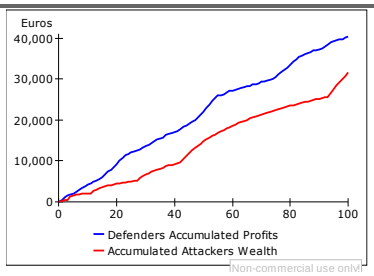
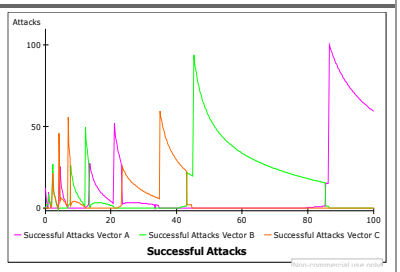
Uncertainty is a multiplier of the unitary cost; this means that there is no uncertainty in the base scenario since uncertainty is equal to 1. Both attackers and defenders know what is the damage (attack unitary cost = 10) that an attack will cause to the information asset through the vector that is being breached.

	Financial Performance	**Successful Attacks**
Scenario #1 Base Scenario		

As shown in the base scenario of the first diagram, attacks are successful starting with A as the start period indicates. However, attackers are switching to the next weakest link whenever the defender fixes the security flaws where the most successful attacks are being reported.

Low Uncertainty

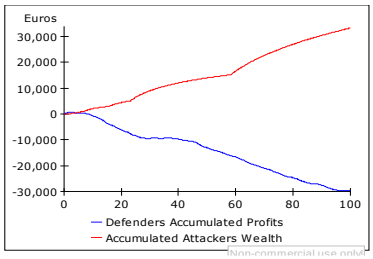
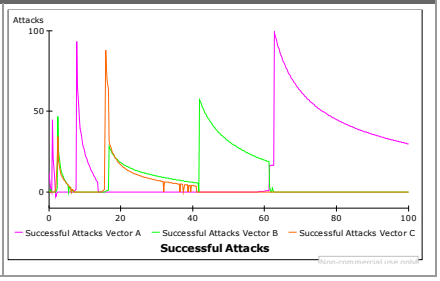
In this case, the Attack Unitary Cost is multiplied by uncertainty U (0.95,1.1). The financial performance of defenders is still growing, although with mild ups and downs. On the other hand, attackers' performance is also unsteadily growing but still performing below defenders' performance, as exhibited in the base scenario.

	Financial Performance	Successful Attacks
Scenario #1 **Low Uncertainty**		

Successful attacks are taking place because of the attacker's weakest link strategy, showing an increase in attacks for vectors B and A at the end of the period peaking to almost 100 attacks.

Medium Uncertainty

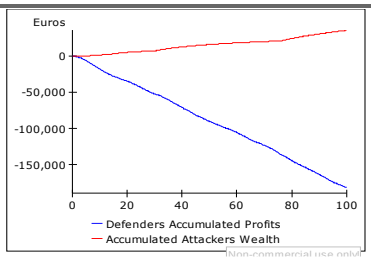
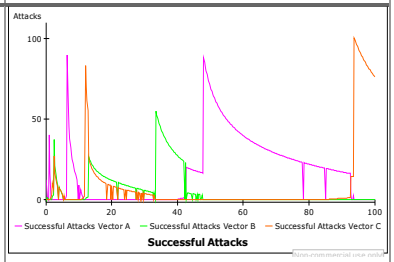
In this case, the Attack Unitary Cost is multiplied by uncertainty U(0.875,1.25). The financial performance of defenders drastically drop below zero, meanwhile attackers continue to perform positively.

	Financial Performance	Successful Attacks
Scenario #1 **Medium Uncertainty**		

Successful attacks continue hitting more intensely the defenses. This time, vector A, B and C are increasing in magnitude, whenever the attacker switches to the next weakest link.

High Uncertainty

In this case, the Attack Unitary Cost is multiplied by uncertainty U(0.75,1.5). Defender's financial performance continues dropping below zero, experiencing even more financial losses. On the contrary, attackers are still performing positively and increasingly.

	Financial Performance	Successful Attacks
Scenario #1 **High Uncertainty**		

Under high uncertainty, all vectors are experiencing successful attacks in a variable way and in high intensity. The previous behavior makes the defender helpless in the way that they cannot distribute their resources effectively since the successful attacks are constantly shifting, making it difficult to just follow the wait-and-see strategy.

7.2.2 Scenario # 2: Asymmetric Capabilities

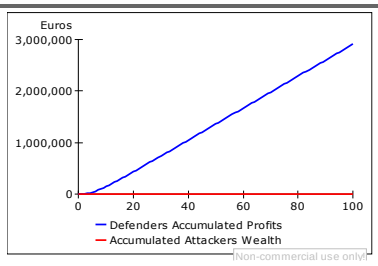
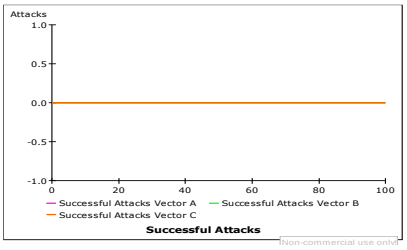
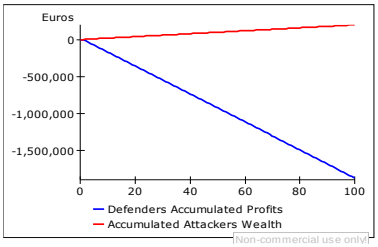
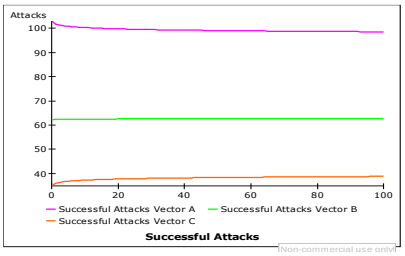
The purpose of this scenario is to show the model's behavior when one of the adversaries have more resources than the other and what is the effect of that behavior in the successful attacks and financial performance of both parties. The following are assumptions treated in the Asymmetric Capabilities scenario:

- Defenders Capabilities are tripled to 3000 Euros.
- Attackers Capabilities are tripled to 300 Attacks.
- Security Vector Values are the same. Vectors A, B and C are equal to 1.

No Uncertainty

When capabilities of defenders are tripled and the attacker's stays the same, the financial performance of the defender is positively increasing, considerably. Meanwhile, when attackers' capabilities are greater than defenders' capabilities, the latter is affected negatively and attackers are benefited.

In the case of successful attacks, if defenders' capabilities surpass the attackers, then there are no successful attacks. By contrast, when attackers' capabilities are higher than defenders, then they will exploit all vectors constantly in the proportion they started attacking since the defender is unable to catch up with attacks. This develops in the same manner even when uncertainty is in place, in all its levels.

	Financial Performance	Successful Attacks
Scenario # 3 Defenders Capabilities> Attackers Capabilities		
Scenario # 3 Attackers Capabilities> Defenders Capabilities		

Low Uncertainty

In this case, the Attack Unitary Cost is multiplied by uncertainty U (0.95,1.1). Defender's financial performance is decreasing negatively. Simultaneously, attackers continue to perform well.

Medium Uncertainty

Here, the Attack Unitary Cost is multiplied by uncertainty U (0.875,1.25). Defender's financial performance continues decreasing negatively and attackers stay being profited.

High Uncertainty

At this point, the Attack Unitary Cost is multiplied by uncertainty U (0.75,1.5). Defender's financial performance drops to even higher negative values. Concurrently, attackers are still being favored since they are superior in capabilities.

If the asymmetries in capabilities between defenders and attackers are substantial, as shown in the graphs, then an increased uncertainty does not make a significant impact on defenders and attackers financial performance or successful attacks.

7.2.3 Scenario # 3: Asymmetric Vector Values

The focus of this scenario is to visualize the impact that different weights in vector values would affect the financial performance of both parties, as well as in the successful attacks. This leads to the question of "What if an attack in certain security vector (which is more valuable) causes more harm than the others to the defender in terms of reputation?". The following are the assumptions applied in the Asymmetric Vector Values scenario:

- Defenders Capabilities and Attackers Capabilities are equal.
- Security Vector Values are asymmetric with values of Max=1.25, Medium=1 and Min=0.75
  - A>B>C
  - B>A>C
  - C>A>B
  - A<B<C
  - B<A<C
  - C<A<B

No Uncertainty

As shown in the graphs, the fact that the defender has asymmetric vector values, does not affect the financial performance of defenders over time. Defender's performance change according to the values assigned to each vector based on the successful attacks breaching them, however, their performance increases and is higher than attackers' performance. Attackers are steadily performing well since they are still being successful on the attacks they are launching.

Similarly, asymmetric vector values do not have any incidence in the successful attacks, since the attackers operate with the weakest link strategy and they switch from vector to vector whenever is profitable to do so. This makes sense given that the profit perceived by the attacker for one successful attack in each vector, is the same regardless of the value such vector has for the defender.

Low Uncertainty

At this point, the Attack Unitary Cost is multiplied by uncertainty U (0.95,1.1). Defenders' performance change according the values assigned to each vector which are the result of the breaches from the weakest link strategy that the attacker is using.

Although, defenders are harmed under low uncertainty, they have the possibility to recover from such harm in most of the cases. The graphs show that when the attackers prefer the most valuable vector for the defender, the initial damage to the defender is substantial. However, the defender has enough time to recover from such damage. When attackers have a second-class preference for the most valuable vector for defenders, a noticeable damage is made in the intermediate zone of the simulation, which does not give enough time to the defender to recover.

Low uncertainty is enough to cause changes in successful attacks quantities which account for negative trends in financial performance of the defender.

Medium Uncertainty

In this case, the Attack Unitary Cost is multiplied by uncertainty U(0.875,1.25). Financial performance for defenders is dropping below zero, as uncertainty is higher, regardless of the value of the vectors.

Under medium uncertainty, the number of successful attacks are present an important increase from low to medium uncertainty. This increase, can explain the aforementioned negative performance of defenders.

High Uncertainty

In this case, the Attack Unitary Cost is multiplied by uncertainty U(0.75,1.5). Defenders' financial performance display pronounced decline across the changes in vector values.

Successful attacks from medium to high uncertainty, the maximum number of attacks in a given vector does not increase much. However, the number of vectors in which the maximum number of attacks are reported, is higher.

Having asymmetries in vector values does not favor the defender in preventing the attackers from eroding defender's reputation. Furthermore, high uncertainty benefits the attackers in defeating defenders much like in the base case scenario.

7.3 Discussion of Implications of Scenario Analysis

As the weakest link strategy is operating in all scenarios, the attacker will prefer the vector with the lowest protection and exploit it until he cannot get more benefits. Meanwhile, the defender is applying the wait-and-see strategy to fix the vulnerabilities according the historical successful attacks. This is effective when there is no uncertainty introduced in the model.

As uncertainty is introduced and/or increased, the benefits to take a wait-and-see approach decreases. Thus, with high uncertainty, the defender is practically acting blindly since the breaches are highly unstable, encouraging the defender to defer investments (or underinvest) and "surrender" preferring to cope with some attacks. This difficulty in decision-making is translated negatively into reputation, hence in financial performance of the defender. The higher the uncertainty, attacks become less intensive in one vector with respect to the others, this means that the defender de-invest in the other vectors.

On the other hand, attackers might change attack strategies. That is, they might not choose to extensively exploit the weakest link to confuse the defender and trigger misallocations of security investments. In fact, there is anecdotal evidence of some spammers, who send waves of messages with no other apparent purpose than to wear out self-learning spam filters (Bohme & Moore, 2009). In this case, attackers may jump from one vector to another without exploiting it completely.

Chapter 8. Policy Options Analysis

This chapter aims to answer the fourth research question. In this chapter, policy options regarded as corporate security management strategies are proposed. Section 8.1 shows Information Sharing as one of the proposed policy options, this policy option aims at reducing uncertainty regarding attacks and increasing the defender's performance; and section 8.2 depicts Higher Dismissal Time of Attacks as the second policy option, which aims at improving defenders' knowledge about attacks and increasing their financial performance as well. Assessments and comments on the implications these policy options are pointed out in the concluding section of the chapter.

8.1 Policy Option 1: Information Sharing

As one of the economic barriers of improving information security is the lack of available data, the argument for sharing information is based on the belief that firms can reduce uncertainty regarding cybersecurity threats, vulnerabilities and, in turn, security breaches; based on the experiences of other (especially similar) firms (Gordon et al., 2015). In the following figure, the information sharing policy option was introduced to the uncertainty section of the model based on the previous scenario analysis construction.

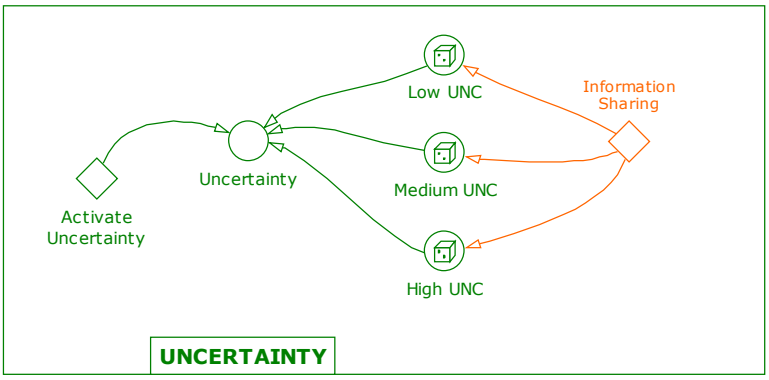


Figure 33 Information Sharing Policy Option

The goal of this piece of structure in the model, is to reduce uncertainty across the simulation period, experiencing a delay of the half of the total simulation time from the moment that the policy is put in place until the perceived benefits are effective.

Figure 34, illustrates how the different levels of uncertainty are working in the model based on their respective ranges:

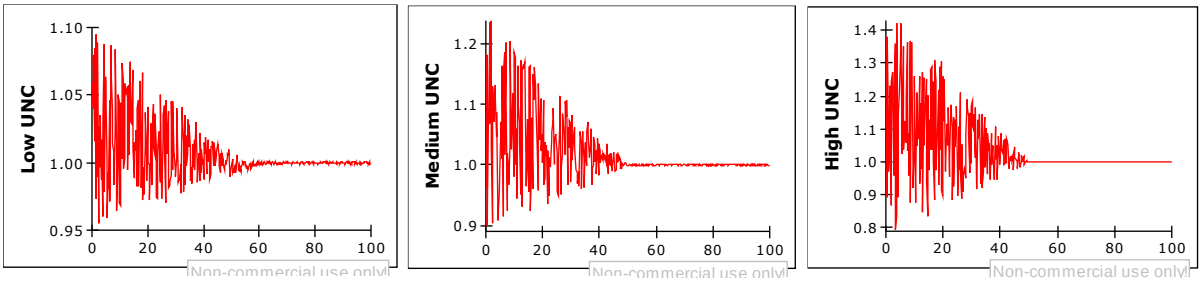
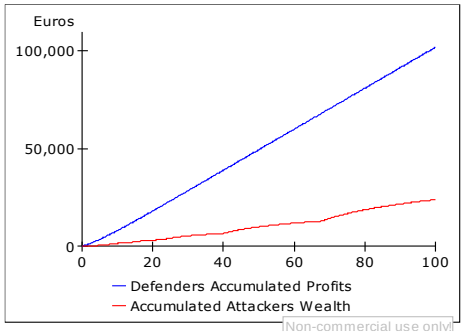
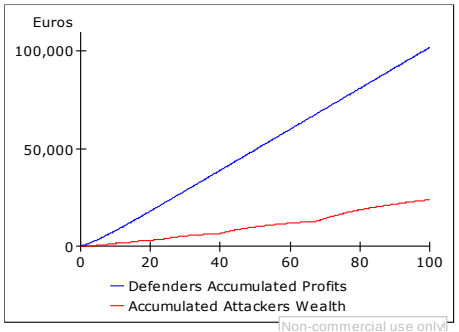
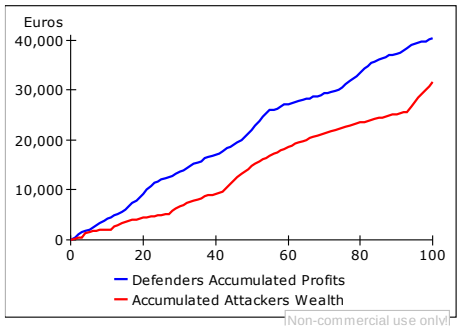
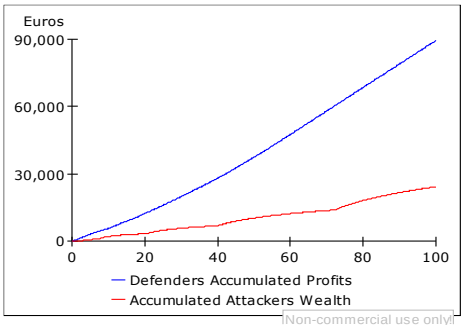
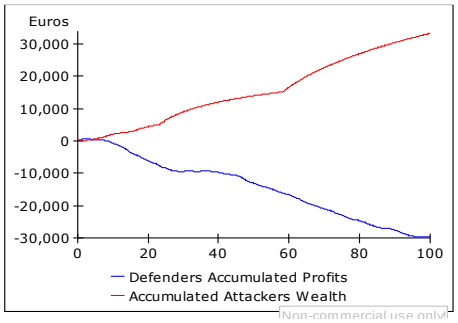
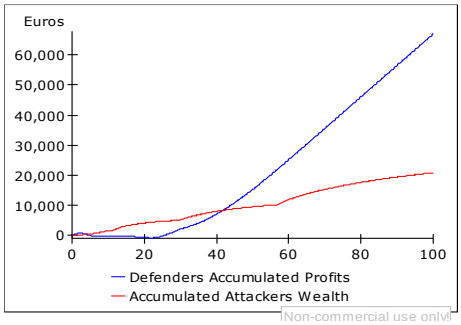
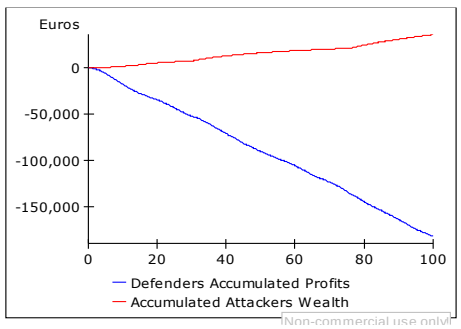
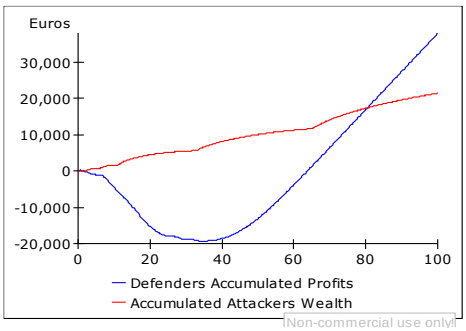


Figure 34 Uncertainty levels with Information Sharing

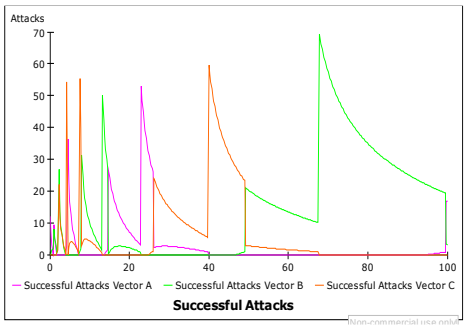
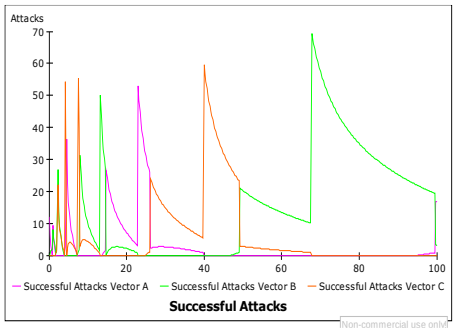
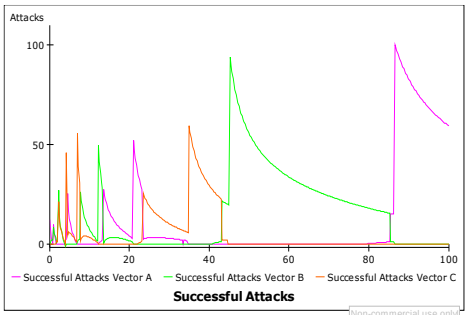
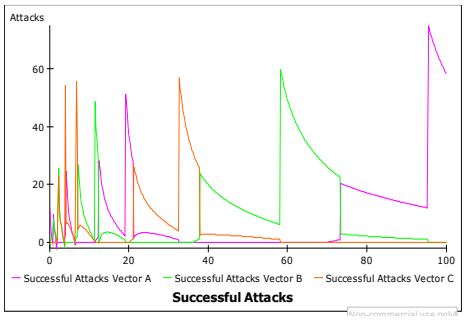
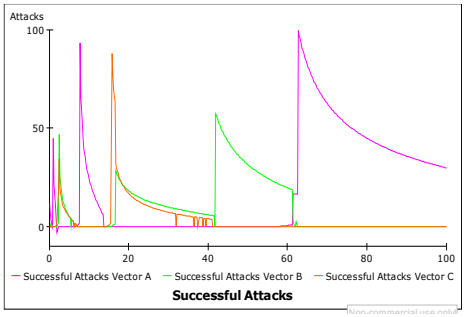
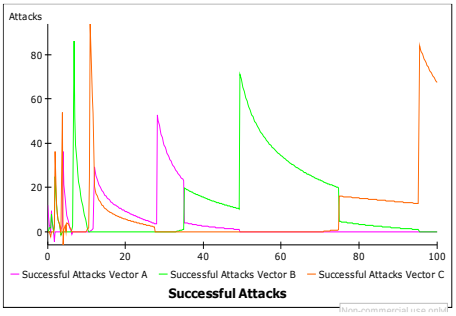
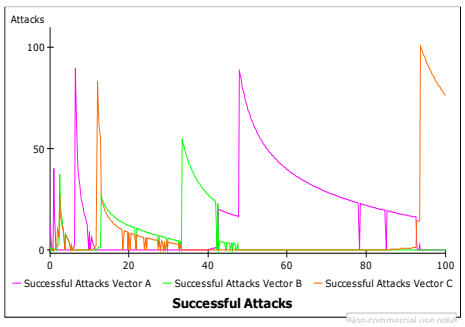
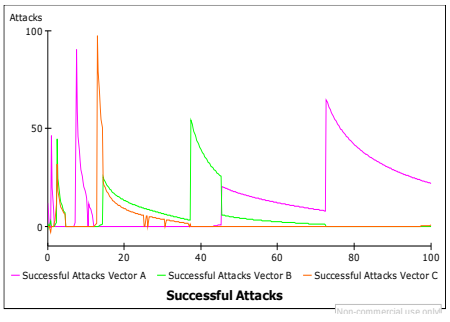
The policy option analysis with Information Sharing is presented with an outline of scenarios followed by two parts:

- The first diagram, shows how this policy option with respect to each change in the level of uncertainty affecting the financial performance of the adversaries.
- The second diagram, illustrates how this policy option influence the successful attacks on each security vector.

8.1.1 Information Sharing Model Behavior: Defender/Attacker Performance

	Without Information Sharing	With Information Sharing
No Uncertainty		
Low Uncertainty		
Medium Uncertainty		
High Uncertainty		

8.1.2 Information Sharing Model Behavior: Successful Attacks

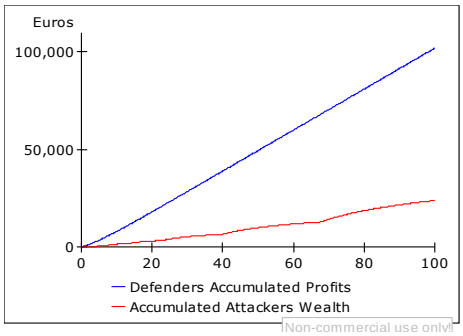
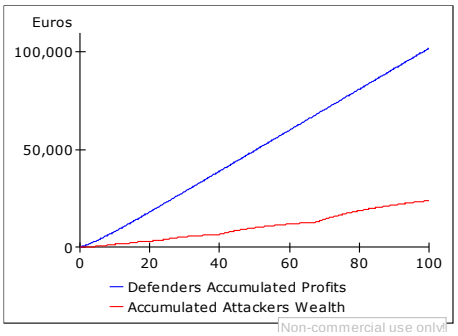
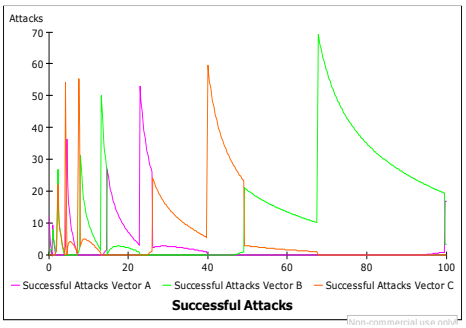
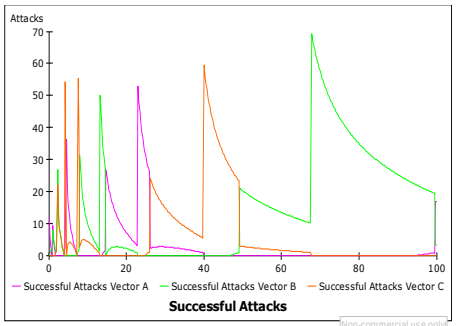
	Without Information Sharing	With Information Sharing
No Uncertainty		
Low Uncertainty		
Medium Uncertainty		
High Uncertainty		

8.1.3 Description of Results for Policy Option 1: Information Sharing

The policy options analysis is simulated with the base run initial conditions and compared with the simulations generated by adding the Information Sharing policy option into the model.

No Uncertainty

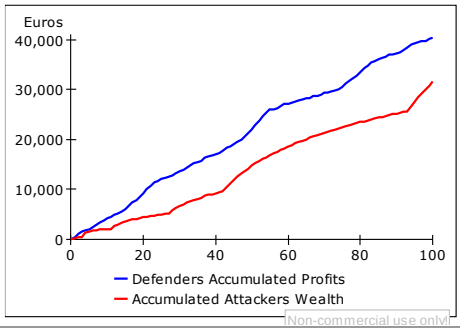
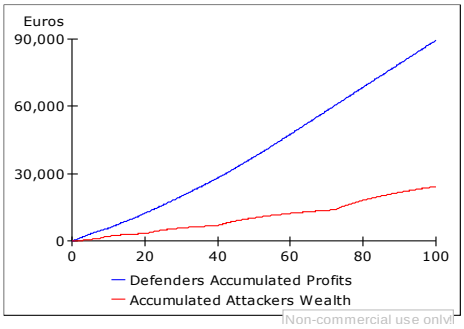
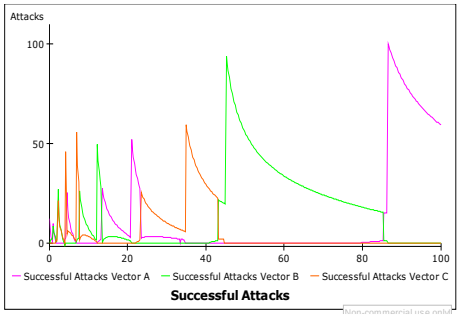
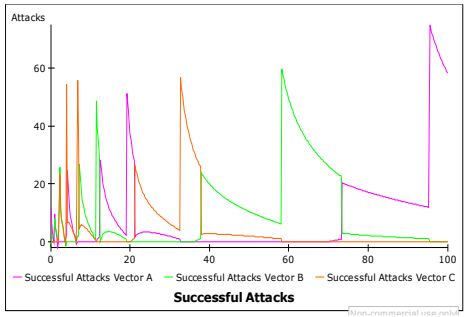
It is clearly seen in the graph that the fact that information sharing policy option is in place, does not affect the financial performance of defenders neither attackers. Similarly, successful attacks do not show any change with this policy. Therefore, the behavior of the system is the same as in the base scenario.

	Without Information Sharing	**With Information Sharing**
Financial Performance		
Successful Attacks		

Low Uncertainty

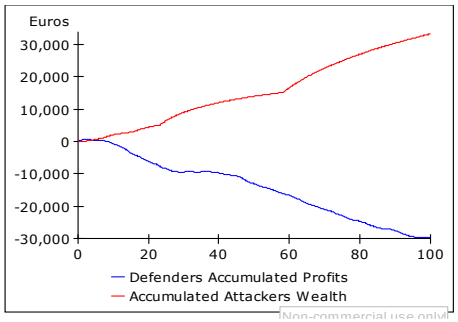
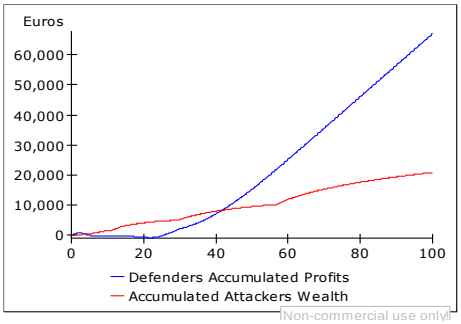
Introducing low uncertainty in the model, it is revealed that with information sharing is reducing uncertainty already and visibly improving the defender's financial performance. Meanwhile attackers' performance remains the same.

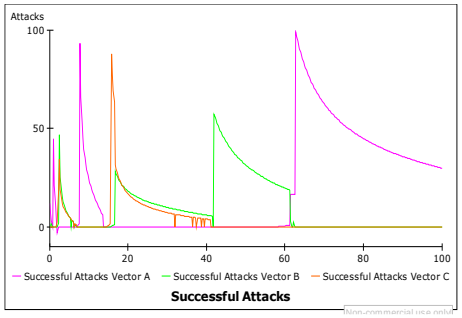
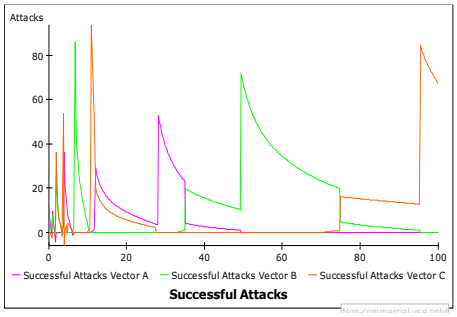
Successful attacks are also reduced in magnitude reaching less than 100 attacks across the simulations.

	Without Information Sharing	With Information Sharing
Financial Performance		
Successful Attacks		

Medium Uncertainty

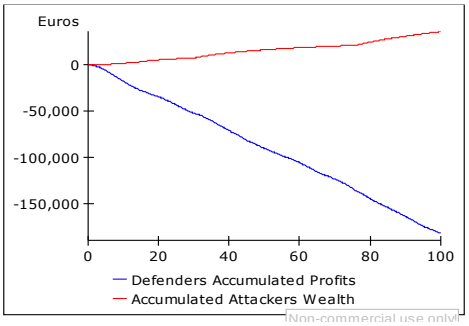
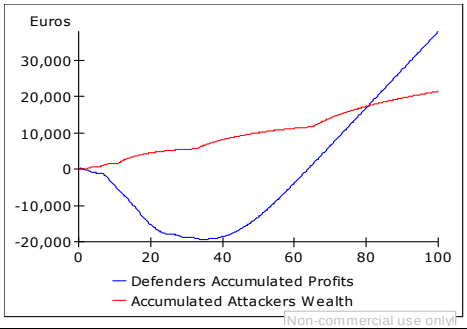
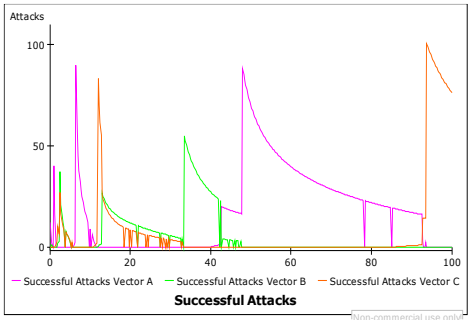
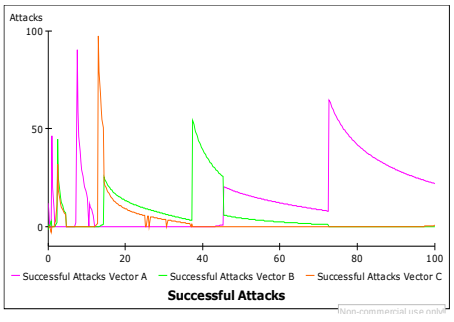
As uncertainty is increasing, it can be observed that financial performance of defenders improving after the first 20 months, surpassing greatly the attackers at the end of the simulation. Defenders are experiencing successful attacks; however, they are able to recover from them.

	Without Information Sharing	With Information Sharing
Financial Performance		

Successful Attacks		

High Uncertainty

With high uncertainty, the defenders' financial performance decreases in the beginning of the simulation until time 40, where it starts increasing increasingly. After time 80, defenders are able to recover and exceed attackers. The Information Sharing effect is also visualized in the successful attacks, attack shifting across the vectors is reduced, allowing defenders to fix the security vulnerabilities and receiving benefits. However, in order for defenders to perceive these benefits they have to wait until this policy option acts in reducing uncertainty.

	Without Information Sharing	**With Information Sharing**
Financial Performance		
Successful Attacks		

8.2 Policy Option 2: Higher Dismissal Time of Attacks

Defenders make investment decisions based on their reported successful attacks. This infers that attacks must be dismissed after some time either because they were resolved or they are simply discarded since they are not relevant. In the base run simulation, the dismissal time of attacks for the defender is one month. Figure 35 shows the dismissal time in the model.

The main purpose of this policy option is to increase the dismissal time of attacks, so the defender "keeps" the reports of successful attacks for longer time in order to learn more from them and eventually reduce uncertainty surrounding future attacks.

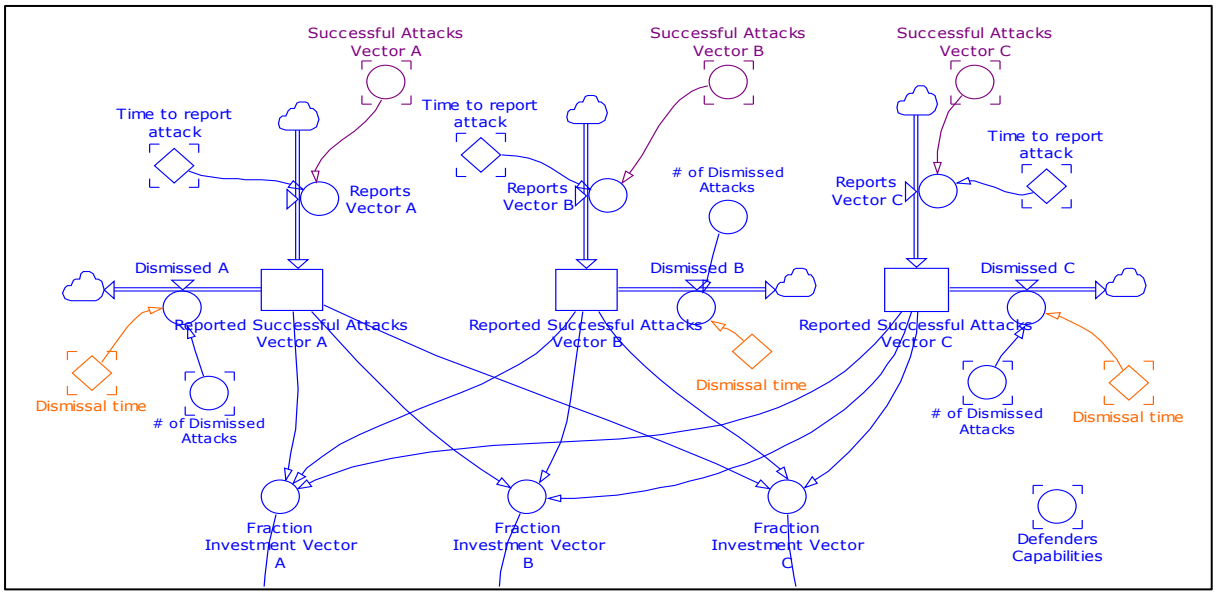


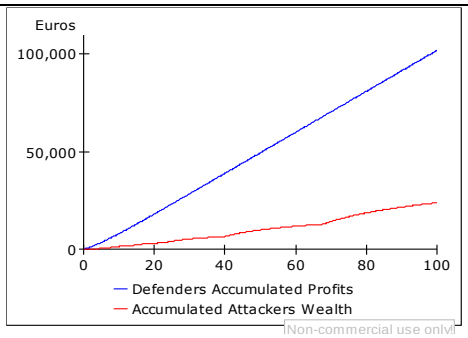
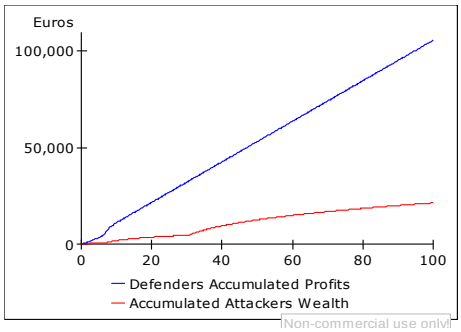
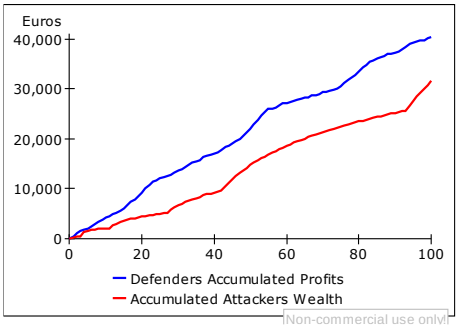
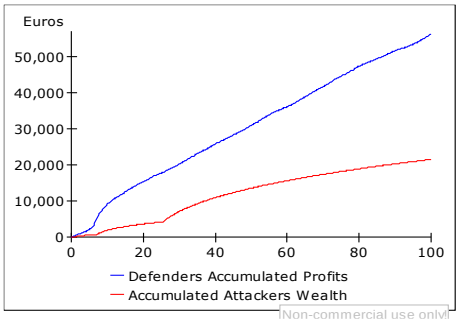
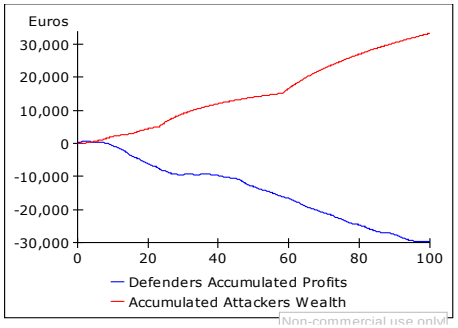
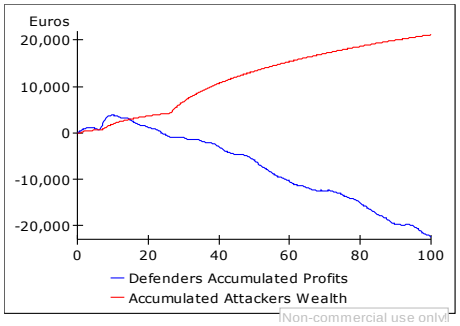
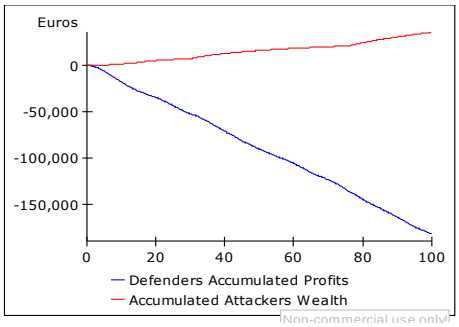
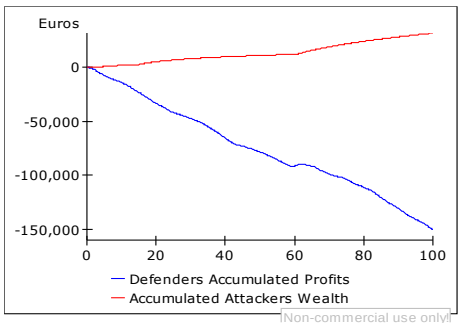
Figure 35 Dismissal Time Policy Option

Before analyzing this policy option, a sensitivity policy parameter test to find the specific time where the uncertainty in the system is reduced and the behavior of the system, improved. The first policy parameter change was to introduce 3 months as dismissal time instead of 1 month. The result of this test showed no improvement in the system's behavior (reducing uncertainty). The second policy parameter test was introducing 4 moths as dismissal time. A tipping point for policy efforts was found in this stage. The system improved defenders' financial performance and successful attacks by reducing uncertainty.

The policy options analysis with higher dismissal time is presented with an outline of scenarios followed by two parts: The first diagram, shows how this policy option with respect to each change in the level of uncertainty affecting the financial performance of the adversaries. The second diagram, illustrates how this policy option influence the successful attacks on each security vector.

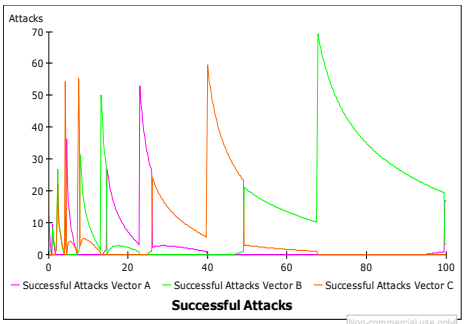
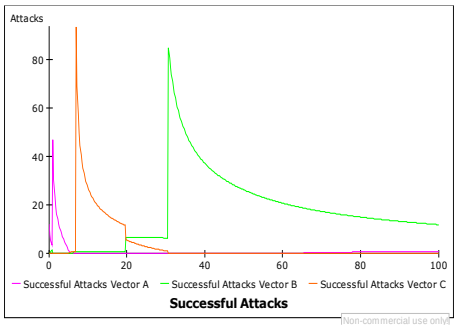
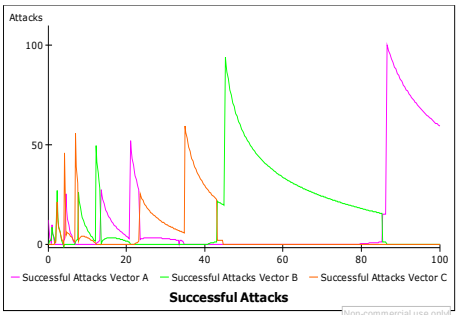
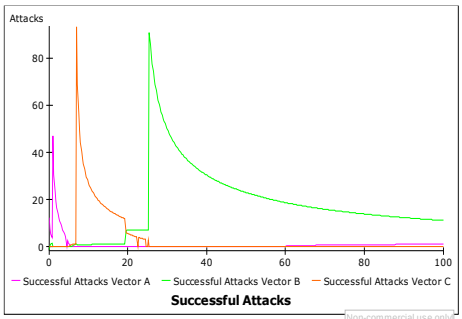
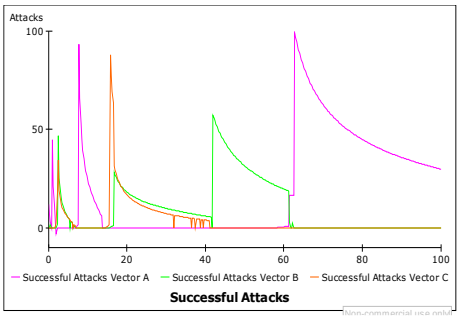
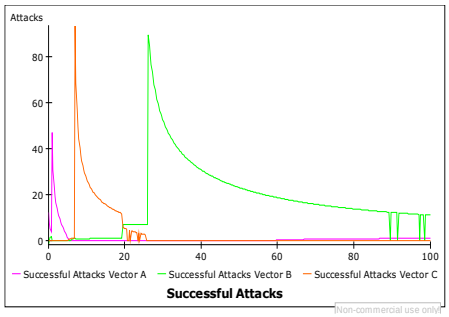
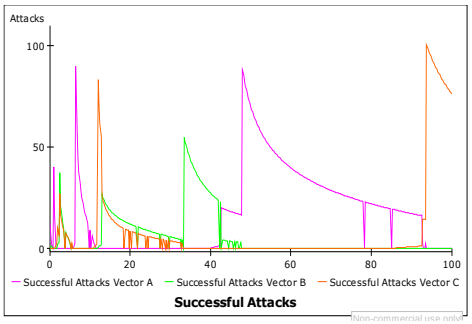
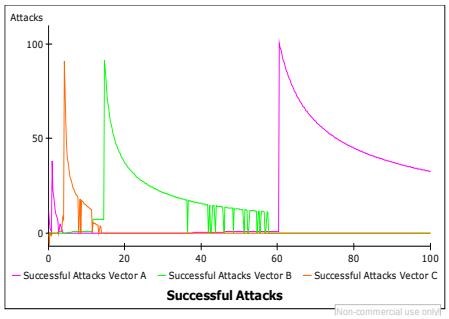
8.2.1 Higher Dismissal Time Model Behavior: Defender/Attacker Performance

Dismissal time = 3 months

	Without Higher Dismissal Time	With Higher Dismissal Time
No Uncertainty		
Low Uncertainty		
Medium Uncertainty		
High Uncertainty		

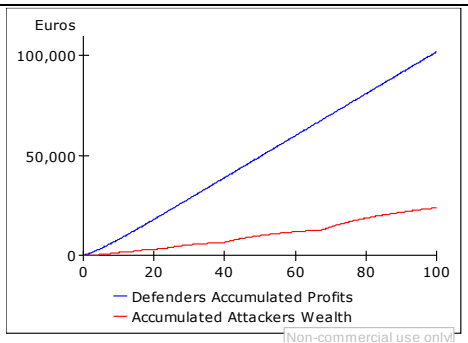
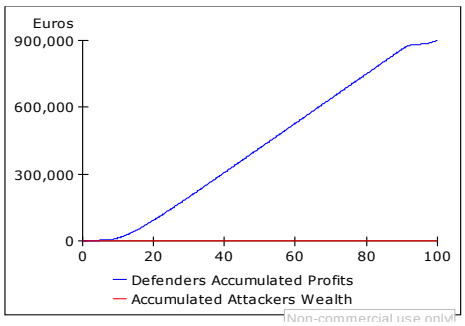
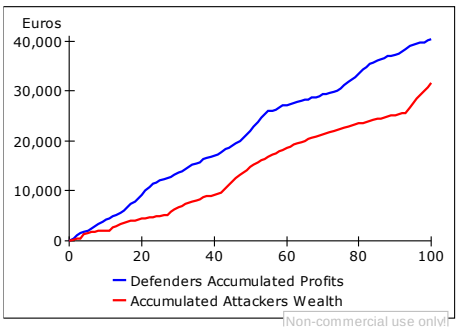
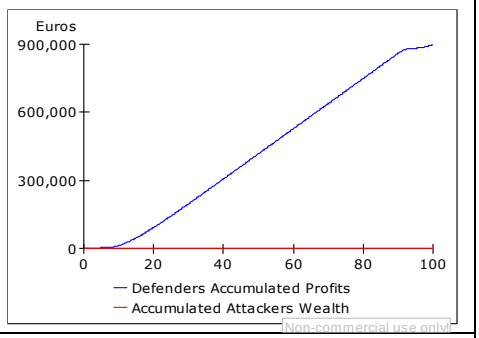
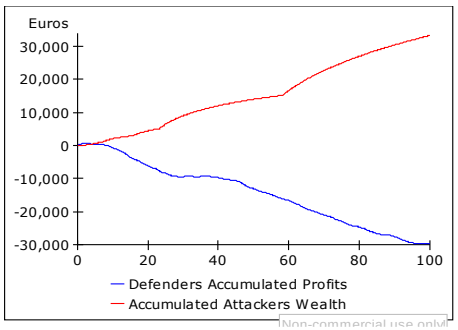
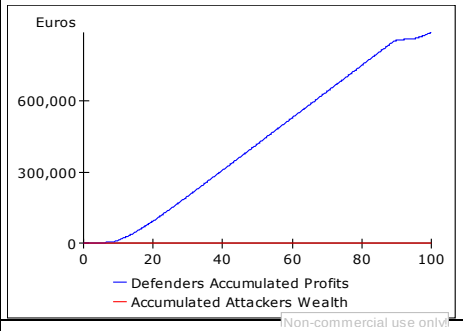
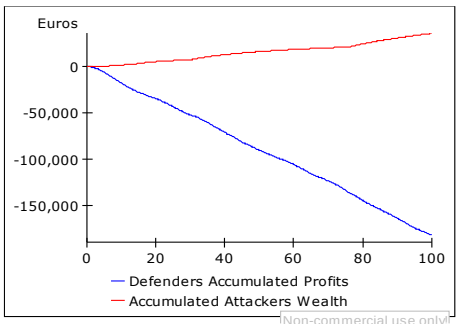
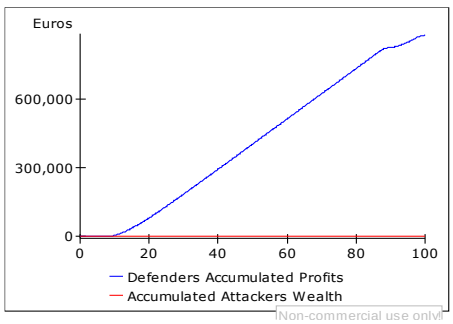
8.2.2 Higher Dismissal Time Model Behavior: Successful Attacks

Dismissal time = 3 months

	Without Higher Dismissal Time	With Higher Dismissal Time
No Uncertainty		
Low Uncertainty		
Medium Uncertainty		
High Uncertainty		

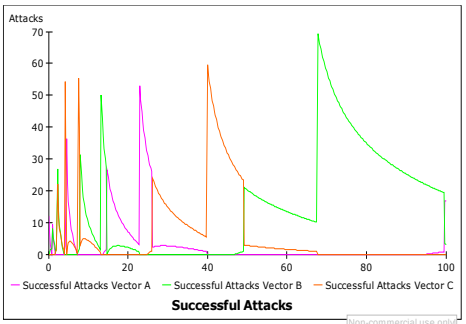
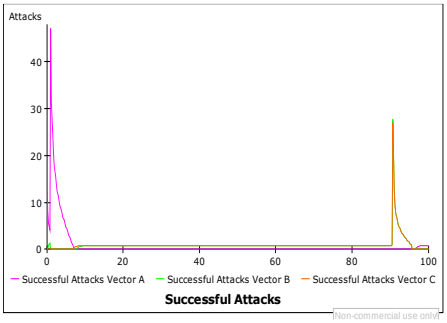
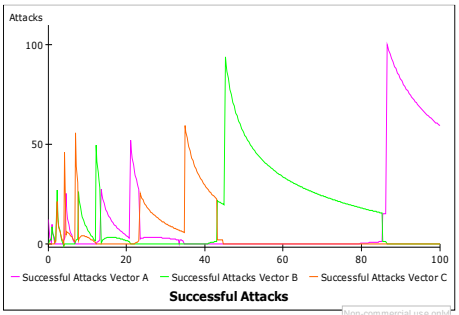
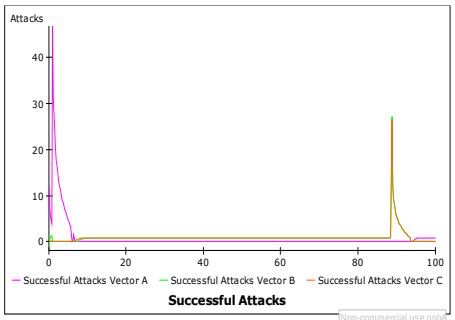
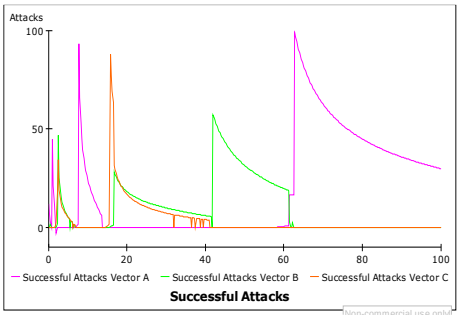
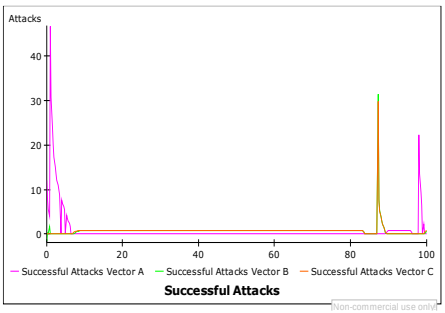
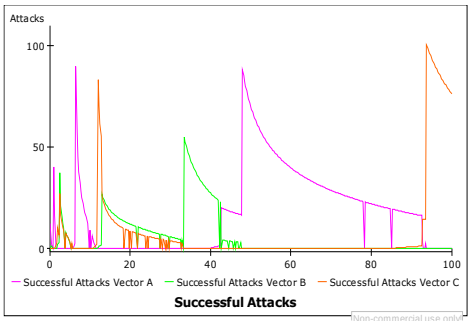
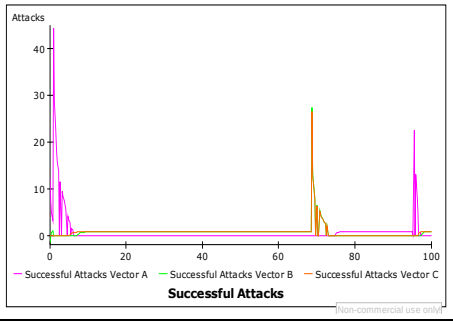
8.2.3 Higher Dismissal Time Model Behavior: Defender/Attacker Performance

Dismissal time = 4 months

	Without Higher Dismissal Time	With Higher Dismissal Time
No Uncertainty		
Low Uncertainty		
Medium Uncertainty		
High Uncertainty		

8.2.4 Higher Dismissal Time Model Behavior: Successful Attacks

Dismissal time = 4 months

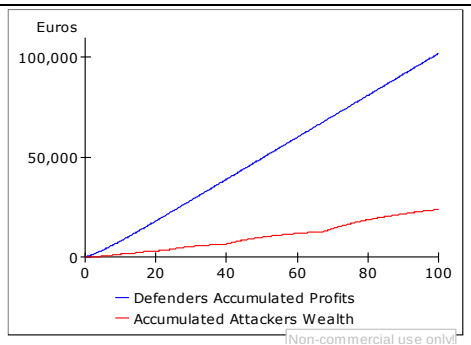
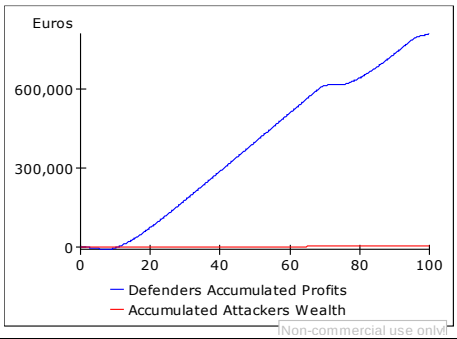
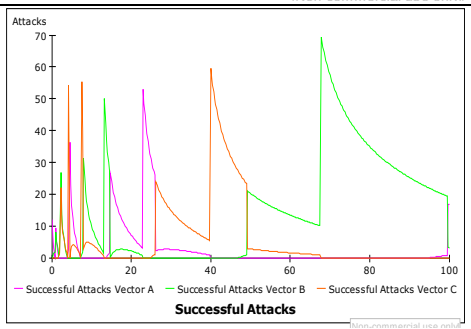
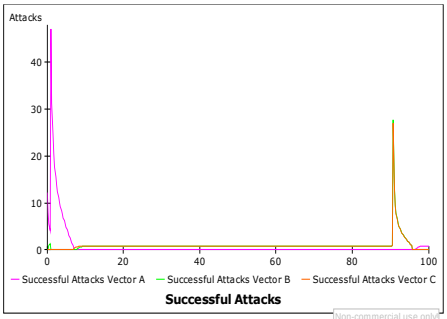
	Without Higher Dismissal Time	With Higher Dismissal Time
No Uncertainty		
Low Uncertainty		
Medium Uncertainty		
High Uncertainty		

8.2.5 Description of Results for Policy Option: Higher Dismissal Time (4 months)

The policy options analysis is simulated with the base run initial conditions and compared with the simulations generated by adding the Higher Dismissal Time policy option into the model.

No Uncertainty

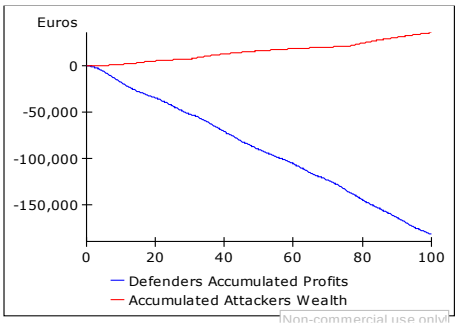
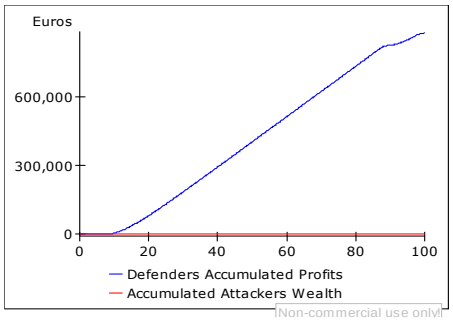
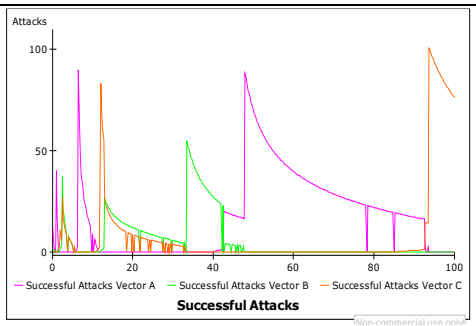
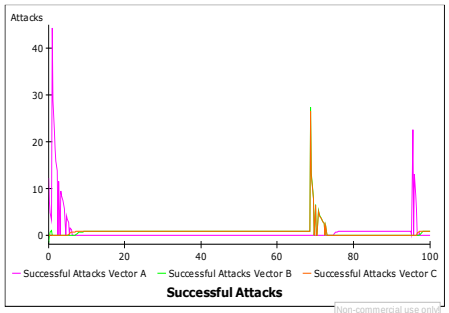
It is visible in the graph that when this policy option is in place, the financial performance of defenders increases meaningfully. On the other hand, attackers' performance remain the same as in the base scenario and considerably below the defenders performance.

	Without Higher Dismissal Time	**With Higher Dismissal Time**
Financial Performance		
Successful Attacks		

Similarly, successful attacks show a drastic change with this policy. The weakest link operates in the beginning of the simulation with successful attacks in Vector A as it is stated in the initial conditions. However, in the following periods, defenders are effectively maintaining the vector's security, not allowing security breaches in any of the three vectors only until the end of the period in Vector C but with less attack intensity.

Low, Medium and High Uncertainty

Introducing uncertainty in the model, it is revealed that with higher dismissal time, the defenders' good financial performance remains increasing in a positive way. Meanwhile attackers' performance remains the same and dramatically lower than defenders. The following table shows the behavior of the system with this policy option under high uncertainty.

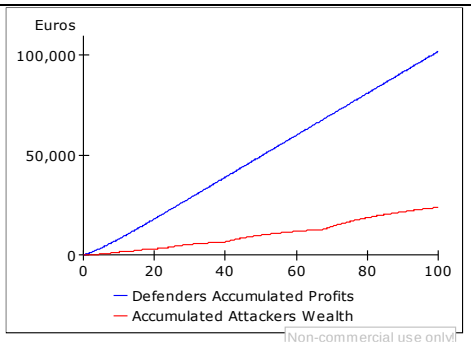
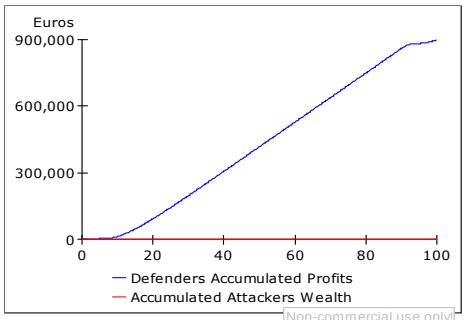
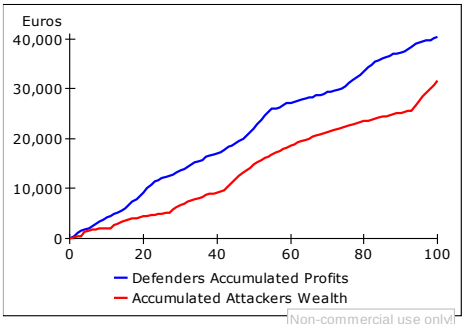
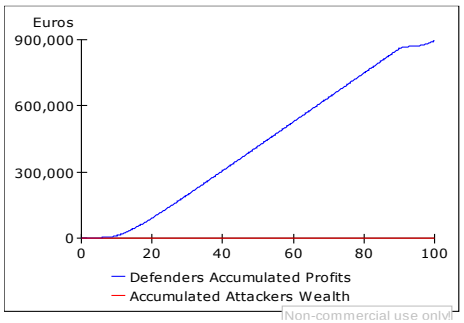
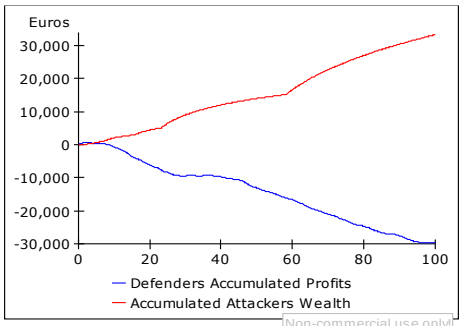
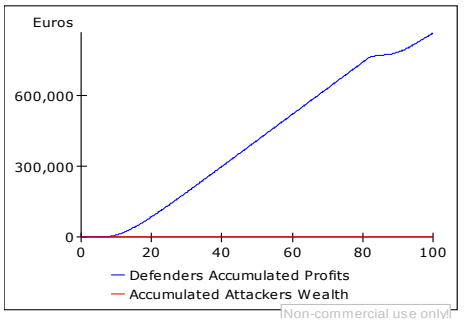
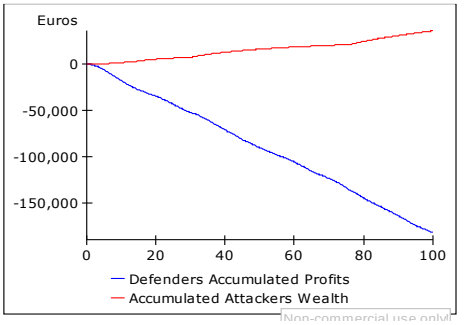
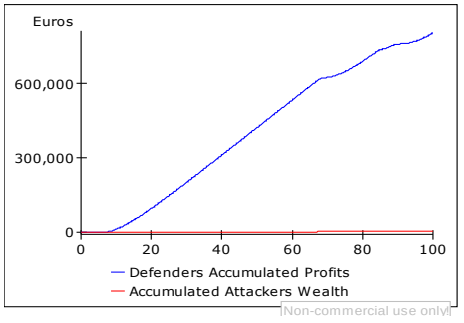
	Without Higher Dismissal Time	**With Higher Dismissal Time**
Financial Performance		
Successful Attacks		

Successful attacks are also reduced in magnitude reaching important levels only in vector A in the beginning (since it is the weakest link) and at the end of the simulation in vector C and A but in lower magnitude. Defenders were able to tackle security breaches in most of the duration of the simulation.

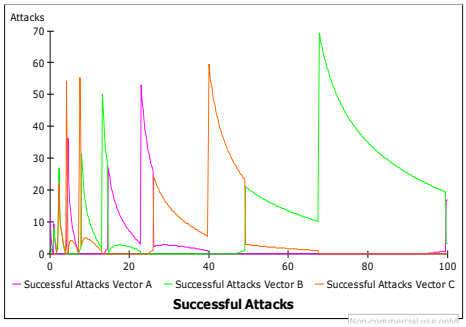
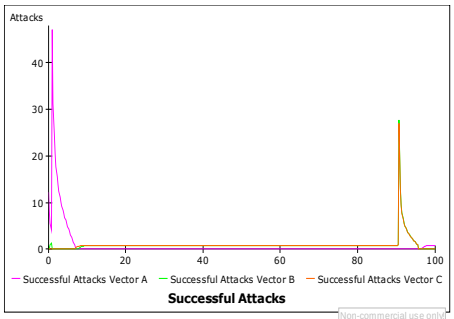
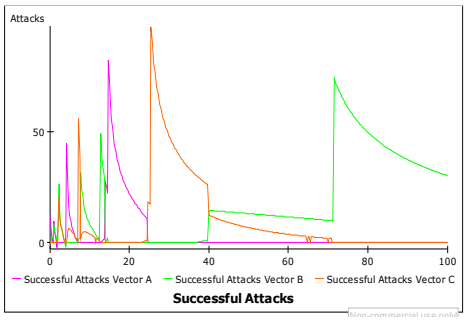
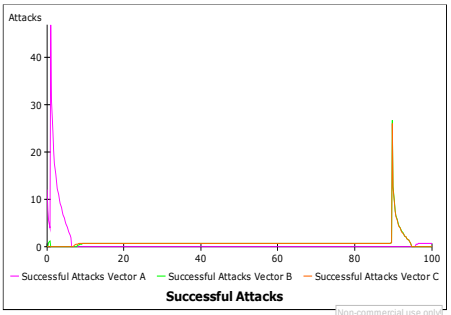
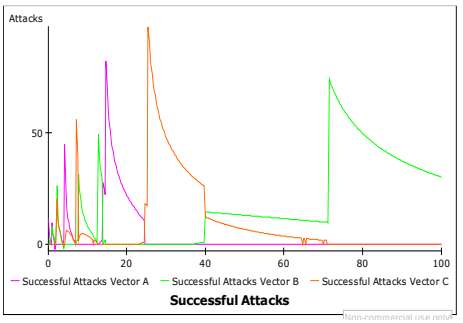
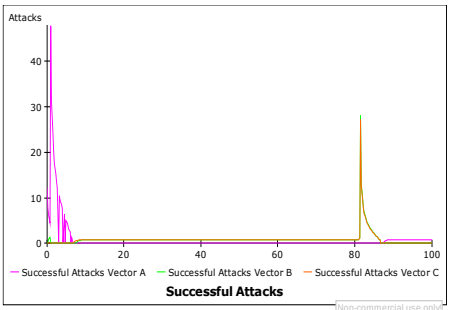
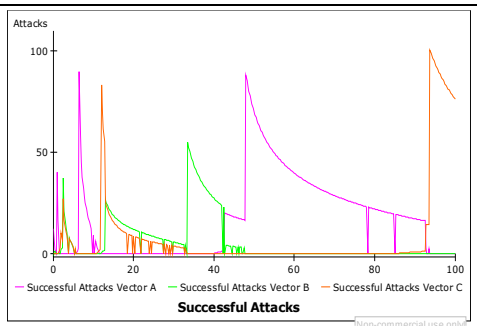
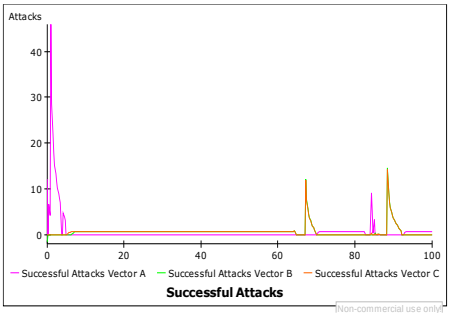
8.3 Combination of Information Sharing and Higher Dismissal time

The next diagrams, present a combination of the two policy options previously exposed. The first diagram shows the financial performance of both Defenders and Attackers and the second diagram shows the behavior of successful attacks.

8.3.1 Combination Model Behavior: Defender/Attacker Performance

	Without Information Sharing nor Higher Dismissal Time	With Information Sharing and Higher Dismissal Time
No Uncertainty		
Low Uncertainty		
Medium Uncertainty		
High Uncertainty		

8.3.2 Combination Model Behavior: Defender/Attacker Performance

	Without Information Sharing nor Higher Dismissal Time	With Information Sharing and Higher Dismissal Time (Dismissal time = 4 months)
No Uncertainty		
Low Uncertainty		
Medium Uncertainty		
High Uncertainty		

8.3.3 Description of Results for Combination of Information Sharing and Higher Dismissal Time

By combining the two policy options, it can be observed in the previous diagrams, that there is an overall improvement on the defense's behalf. Defenders' financial performance is significantly superior to attackers and increasing and successful attacks are mostly mitigated by the defender throughout the periods, especially under high uncertainty.

8.4 Discussion of Implications of Policy Options Analysis

8.4.1 Policy Option 1: Information Sharing

Information sharing has the potential for reducing uncertainty surrounding information security investment decisions. As a result of this reduction in uncertainty, information sharing is likely to lessen the common tendency by firms to wait for a major breach in information security before investing significant funds for security activities. In other words, Information sharing encourages firms to take a more proactive, compared to a reactive approach towards cybersecurity investments. Thus, the value to take a wait-and-see approach decreases as the uncertainty associated with the investments increases.

First, it was illustrated that under medium and high uncertainty, the defender's financial performance experience a worst-before-better behavior regarding their recovering from security breaches. This suggests that defenders should be patient to perceive the benefits of information sharing, this finding makes sense since it takes time for the information collection and gathering to be completed. Furthermore, this information requires time to be analyzed and understood by the security staff and for security managers to make investment decisions. Also, an increase in the defense's benefits is clearly seen in the graphs, which should encourage firms to share their information in return for receiving information from other firms. This can also offset the costs typically associated with belonging to an information-sharing group (Gal-Or & Ghose, 2005).

While the analysis of this study showed that information sharing does indeed offer the potential to reduce overall uncertainty revolving information security, there are some pitfalls that may well prevent the realization of the full potential benefits. One of these pitfalls is the prevalence

of free-riding members in the information sharing group. Emerging free-riding[10] in an information-sharing group is one of the major reasons why firms are reluctant to share cybersecurity information (Gordon et al., 2003b).

Another obstacle for a firm to share its information regarding cyber security is taking risk to compromise the firm's competitive advantage by disclosing security weaknesses. Accordingly, Gal-Or & Ghose (2005) and Gordon et al. (2003b) remark that although information sharing's pitfalls revolve around the need to create economic incentives to facilitate effective information sharing (p.481) such as insurance risk premium, bug challenge and bounty, etc.

8.4.2 Policy Option 2: Higher Dismissal Time

Increasing the dismissal time of successful attacks has managerial implications. For example, by keeping the information regarding reported successful attacks for 4 months instead of 1 month, firms may experience the need of specialized staff to analyze the collected data, incur in costs for data warehousing infrastructure, assign a response (IT Forensics) team with all competencies, and to have an integrated system to collect data.

If there is no uncertainty, a defender can still perform well following a standard wait-and-see approach. As soon as uncertainty arises, the more valuable the information gained from observed attacks is. This means that defenders become more proactive when uncertainty is high.

8.4.3 Combination of two policy options

Individually, each policy improves the financial performance of defenders over time. However, information sharing reduces uncertainty but it entails a more delayed success than increasing the dismissal time of attacks, financial performance of defenders with information sharing suffer losses in the first half of the period. Apart from the late success in reducing uncertainty, information sharing carries several obstacles to be executed in the first place, such obstacles

10 The free rider problem refers to a situation where a firm can benefit from a situation irrespective of the magnitude of the firm's contribution. See Varian (2002) for an analysis of how the free-rider problem affects decisions to invest in cybersecurity.

include the free-rider problem, regulations and mostly lack of economic incentive to belong to an information sharing group since most firms are hesitant to expose their security weaknesses to their competitors indicating a market disadvantage even though a coordinated view of attacks could prompt faster mitigation to everyone's benefit.

Meanwhile, increasing the dismissal time of attacks on its own, present an almost immediate success allowing to analyze deeply the reported successful attacks for longer time. This policy clearly improves the financial performance for defenders and diminish successful attacks. However, this is the policy option that involves the more need of resources since it requires integrated infrastructure and specialized response staff (IT Forensics) to be able to collect analyze and storage information about attacks for 4 months.

Implementation of the combination of information sharing and higher dismissal time depends on the size of the firms and the available budget (capabilities) to invest in information security. As it was observed in the combined policy simulations, there is small added value in combining the two policies since defenders can perceive benefits in different ways by implementing just one policy at the time. The dismissal time policy results seem to be just as good as the combined policy. In other words, the marginal benefit of information sharing is seemed to be practically zero if the dismissal time policy is already in place.

Therefore, firms that are smaller may opt to be part of an information sharing group, especially if these are similar firms, since it required less budget to reduce uncertainty. The greater the similarities among the firms, the more likely the information shared will be accurate and valuable in terms of reducing uncertainty. On the other hand, greater firms might be motivated to put higher dismissal time policy in place since they are more likely to dispose a higher budget to implement this policy. Plus, big firms can avoid the pitfalls of belonging to an information sharing group and protecting their general reputation.

Chapter 9: Conclusions

This study presented a System Dynamics model with endogenous investment decisions between two adversaries in the information security field. The model was built to better understand the dynamic investment decision strategies evoked by defenders and attackers. Scenarios and policies were tested to explore the implications of investment strategies under uncertainty. The conclusions of this work comprise the answer of the research questions and limitations which are shown thereafter.

9.1 Answer to Research Questions

Chapter 1 depicted an introduction to the current problematic situation of information security, motivated its importance and served as means to focus on one of its major pressing issues, security investments. This chapter also introduced the research objective and research questions that would be addressed by this thesis. To summarize, the objective of this thesis project is to first, understand the dynamic interactions between defenders and attackers when making information security investment decisions, and second, derive the main implications of two theoretical frameworks from information security investment literature: The Wait-And-See approach for defenders and the Weakest Link approach for attackers. A System Dynamics model to study investment strategies derived from such theories was built. The model is also utilized to identify and assess possible policy leverage points to mitigate the effects inherent in such analysis.

Chapter 2 described the chosen methodology to develop the objective of this thesis. It was explained why System Dynamics is an appropriate methodology to represent the dynamic mechanisms of information security investments. In addition, the data collection and analysis process was described in detail.

Chapter 3 provided an overview of the existing literature which the answer to the first research question (What are the relevant concepts and variables and relationships described in Wait-And-See and Weakest Link theoretical frameworks?). This chapter provided a detailed explanation of the previous research carried out by scholars and experts in the information security investments field. It was through the systematic literature review that the factors driving information security investment and how these factors in turn depend on the outcomes such investment, were understood and translated into a stock and flow diagram and a causal loop diagram.

Chapter 4 focused on representing the dynamic interactions between attackers and defenders in a System Dynamics model. This Chapter answered the second research question (How can existing theories defined in WAS and WL be represented in a System Dynamics framework?) To answer this research question, the WAS and WL theoretical frameworks were integrated in a causal loop diagram (CLD). The CLD described two main feedback loops: a reinforcing loop operating in the Weakest Link strategy where an increase in successful attacks leads to more attacks from the attacker, therefore, an increase in vulnerability in security vectors; and a balancing loop operating with the Wait-and-see strategy where an increase in successful attacks, yields more investments from the defense so there is a reduction in vulnerability of security vectors. As the two investment strategies were integrated into a system dynamics simulation model, chapter 4 also explained in detail how these mechanisms interact with each other, as well as explicitly stated the assumptions supporting the model.

Chapter 5 described the behavior of the system by means of the analysis of the base run and equilibrium run, answering the third research question (What are the dynamic implications of WAS and WL theories in the SD model?). The system behavior in the base run showed the weakest link and wait-and-see strategies operating. It was observed that attackers are constantly finding the weakest link and exploiting it, meanwhile the defenders are fixing the defense flaws as the attacks happen. The financial performance of both defenders and attackers is visualized while each party is applying their investment strategy.

Chapter 6 established the model's validity and provided strengthened confidence both in its qualitative and quantitative results. This strengthened confidence was supported by the coherent and consistent way the key variables of the model such as initial conditions of accumulated successful and defender/attacker capabilities, were related to each other. The simulation of these key components resulted in adequate behavior when compared to the knowledge available for comparison in the real system.

Chapter 7 answered the fourth research question (What are the dynamic implications for investment decisions in information security under different uncertainty level scenarios?). Through the delimitation of three different scenarios, conditions such as asymmetries in capabilities and in vector values played an important role when analyzing the behavior of financial performance of defenders and attackers and successful attacks under low, medium and high uncertainty compared with the base scenario.

In this regard the answer to the fourth research, can be given along the line that if uncertainty is high, a defender surrenders and prefers to cope with attacks. High uncertainty can demotivate security investments since defenders are deciding practically blind folded and attackers might not choose to fully exploit the weakest link to confuse the defender and trigger misallocations of security spending.

After the detail scenario analysis, Chapter 8 addressed the fifth research question (What policy options can be identified and what are their dynamic implications?). Two policy options that could reduce uncertainty and improve financial performance regarding information security, were identified. These policies were evaluated in terms of their effects in financial performance of both opponents and in successful attacks. To conclude this chapter, a brief discussion of the possible implications of the implementation of such policies, was brought to attention.

The policy dimension of this study is to allow ways to reduce or cope with uncertainty. This can be done by including information gathering with other defenders and/or increasing the dismissal time of successful attacks. The demonstrated benefit gained from information sharing could provide the necessary incentive to overcome firms' reluctance to actively share their private information. However, defenders experience a worst-before better behavior in their financial performance, suggesting that they should be patient when implementing this policy options since the benefits will be perceived after some time. The second policy option, seems to be more promising in terms of immediacy of results, though there are managerial implications that need careful consideration when selecting this policy option. A combination of policies is possible as shown in the analysis, giving advantageous results for defenders. There are key characteristics to consider in this regard: the average size of firms and the budget available to invest in information security.

All in all, the model developed in this study helped identify influential factors, notably uncertainty about attacks, so that incentive-based security countermeasures can be derived. The presentation of the model behavior in a scenario and policy space, provides support to employ system dynamics as a powerful tool to examine information security investment analysis.

9.2 Limitations and Further Work

As with most research related to information security, the research contained in this thesis has its limitations.

- A natural extension of the research would be to empirically test the conceptual arguments presented in this thesis. One way to conduct such a test would be via a laboratory experiment, where the participants play as corporate managers in charge of cybersecurity activities within their firms.
- The current research effort based the decision rules of attackers and defenders on robust assumptions or best available data. All data sources regarding information security investments were distilled from literature, scientific articles, reports, among others. By conducting case studies of cybersecurity investment decisions by actual firms using their records and mental models, would represent another way to empirically test the arguments of this thesis and would prove valuable in terms of validating the resulting model.
- Since the capabilities of both adversaries were modelled as exogenous parameters, it would be interesting to expand the boundaries of the model to include the dynamics of the financial mechanism undergoing in the defenders and attackers, endogenously. This would prove have a great value in identifying other feedback loops concerning capabilities and corresponding policy options to improve the defender's performance.
- Another limitation of this study is that the model is lacking of financial indicators and analyses such as: cost-benefit analysis, Annual Loss Expectation (ALE), Return on Security Investment (ROSI), Net Present Value (NPV), etc.; to complement the existing assumptions and make the model more comprehensive, further research would be needed to accomplish this.
- The current level of aggregation of the simulation model is adequate for pinpointing fundamental leverage points at a conceptual level; though it does not allow for precise estimates that could lead to the design of policies that could be put into action. Disaggregating and detailing the model to test the policies would be necessary step to following in this regard.

The above limitations notwithstanding, this research provides an important step in helping firms better understand the dynamic interactions of defenders and attackers when making investment decision related to cybersecurity activities.

References

Scientific references, Books and Reports:

Anderson, R. (2001). Why information security is hard - An economic perspective. *Proceedings - Annual Computer Security Applications Conference, ACSAC, January*, 358–365.

Anderson, R., & Moore, T. (2006). The Economics of Information Security : A Survey and Open Questions. *Science*, *314*(October), 610–613. http://doi.org/10.1126/science.1130992

Arora, A., Hall, D., Piato, C. A., Ramsey, D., & Telang, R. (2004). Measuring the risk-based value of IT security solutions. *IT professional*, *6*(6), 35-42.

Axelrod, R. (2003). Advancing the Art of Simulation in the Social Sciences. *Japanese Journal for Management Information Systems*, 12(3), 1–19

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers don't go for cyber-insurance products. *Communications of the ACM*, *52*(11), 68.

Bandyopadhyay, T., Jacob, V.S., & Raghunathan, S. (2005). Information Security Investment Strategies in Supply Chain Firms: Interplay Between Breach Propagation, Shared Information Assets and Chain Topology. *Eleventh Americas' Conference on Information Systems.* URL: http://aisel.aisnet.org/amcis2005/456/.

Barlas, Y. (1989). Multiple Tests for Validation of System Dynamics Type of Simulation Models. *European Journal of Operations Research*, 42, 59–87.

Barlas, Y. (1996). Formal aspects of model validity and validation in system dynamics. *System Dynamics Review*, *12*(3), 183–210.

Barlas, Y., & Erdem, A. (1994). Output Behavior Validation in System Dynamics Simulation. In *Proceedings of the European Simulation Symposium*, Istanbul, Turkey, 81-84.

Behara, R., Huang, C. D., & Hu, Q. (2007). A System Dynamics Model of Information Security Investments. In *Proceedings of European Conference on Information Systems*, 1572–1583. Geneva.

Bier, V., Oliveros, S., & Samuelson, L. (2007). Choosing what to protect: Strategic defensive allocation against an unknown attacker. *Journal of Public Economic Theory*, *9*(4), 563–587.

Bodin, L., Gordon, L., & Loeb, M. (2005). *Evaluating Information Security Investments Using Analytical Hierarchy Process*. *Communications of the ACM,* 48(2), 79-83.

Böhme, R., & Felegyhazi, M. (2010). Optimal information security investment with penetration testing. In *Decision and Game Theory for Security*. Berlin, Springer Berlin Heidelberg, 21–37.

Böhme, R., & Moore, T. (2009). The Iterated Weakest Link A Model of Adaptive Security Investment. In *Workshop on Economics in Information Security*, 24–25. London.

Böhme, R., & Nowey, T. (2008). Economic security metrics. In *Dependability Metrics: Advanced Lectures*, 176–187. http://doi.org/10.1007/978-3-540-68947-8_15

Bojanc, R., & Jerman-Blažic, B. (2008a). Towards a Standard Approach for Quantifying an ICT Security Investment. *Computer Standards & Interfaces*, *30*(4), 216–222.

Bojanc, R., & Jerman-Blažic, B. (2008b). An Economic Modelling Approach to Information Security Risk Management. *International Journal of Information Management*, *28*(5), 413–422.

Buck, K., Das, P., & Hanf, D. (2008). Applying ROI Analysis to Support SOA Information Security Investment Decisions. In *IEEE Conference on Technologies for Homeland Security*, (pp. 359–366).

Casella, G., & Berger, R. L. (2002). *Statistical Inference* (Second ed.). Pacific Grove, CA: Thompson Learning Inc.

Cavusoglu, H., & Raghunathan, S. (2004). Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches. *Decision Analysis*, 1(3), 131–148.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, 47(7), 87–92.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The Value of Intrusion Detection Systems
in Information Technology Security Architecture. *Information Systems Research*, 16(1), 28–46.

Cavusoglu, H., Raghunathan, S., & Yue, W.T. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, 25(2), 281–304.

Coyle, G. (2000). Qualitative and quantitative modelling in system dynamics: some research questions. *System Dynamics Review Autumn*, *16*(3), 225–244.

Cremonini, M., & Nizovtsev, D. (2006). Understanding and Influencing Attackers' Decisions : Implications for Security Investment Strategies. *Workshop on the Economics of Information Security (WEIS)*, 1–24. http://doi.org/10.1145/99977.99985

Davis, A. (2005). Return on security investment – proving it's worth it. *Network Security*, 11,8–10.

De Gooyert, V. (2016). Nothing so practical as a good theory; Five ways to use system dynamics for theoretical contributions. In *Proceedings of the 34th International Conference of the System Dynamics Society*. Delft, The Netherlands: System Dynamics Society.

Denscombe, M. (2012). *Research Proposals: A Practical Guide*. Maidenhead: Open University Press.

Drisko, J. (2003). Improving sampling strategies and terminology in qualitative research. *Paper presented at the Society for Social Work and Research Annual Meeting*. Washington, DC.

Ford, A. (2010). *Modeling the Environment* (Second ed.). Washington, DC: Island Press.

Forrester, J.W. (1961). *Industrial dynamics.* Cambridge: MIT Press.

Forrester, J. W. (1992). Policies, decisions, and information sources for modeling. *European Journal of Operational Research, 59*, 42-63.

Forrester J.W., Senge P. (1980). Tests for building confidence in system dynamics models. *TIMS Studies in the Management Sciences, 14*, 209–228.

Gal-Or, E., Ghose, A., (2005). The economic incentives for sharing security information. *Information Systems Research*, 16(2), 186–208.

Gao, X., Zhong, W. & Mei, S. (2013a). A differential game approach to information security investment under hackers' knowledge dissemination. *Operations Research Letters*, 41(5), 421–425.

Gao, X., Zhong, W. & Mei, S. (2013b). Information Security Investment When Hackers Disseminate Knowledge. *Decision Analysis*, 10(4), 35–368.

Gartner (2011). *Magic Quadrant for Security Information and Event Management*. Gartner RAS Core Research.

Gartner (2012). *IT Key Metrics Data 2012: IT Enterprise Summary Report*. Gartner RAS Core Research.

Geletkanycz, M., & Tepper, B. J. (2012). From the editors. Publishing in AMJ - Part 6: Discussing the implications. *Academy of Management Journal*, *55*(2), 256–260. http://doi.org/10.5465/amj.2012.4002

Greenberger, M., Crensen, M.A., Crissy, B.L. (1976). *Models in the Policy Process*. New York: Russell Sage Foundation.

Gordon, L. A. (2000). *Managerial Accounting: Concepts and empirical evidence (Fifth ed.).* McGraw-Hill.

Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457.

Gordon, L. A., & Loeb, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, *49*(1), 121–125.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003a). Information security expenditures and real options: a wait-and-see approach. *Computer Security Journal*, *19*(2), 1–7.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003b). Sharing information on computer systems security: an economic analysis. *J. Account. Public Policy,* 22 (6), 461–485.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment : A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519.

Grossklags, J., Christin, N., & Chuang, J. (2008). Secure or insure?: a game-theoretic analysis of information security games. *Proceeding of the 17th International Conference on World Wide Web*, *7*(1), 209–218. http://doi.org/10.1145/1367497.1367526

Größler, A., Thun, J.H. & Milling, P.M. (2008). System Dynamics as a Structural Theory of Strategic Issues in Operations Management. *Production and Operations Management*, 17(3), 373–384

Hausken, K. (2006). Income, interdependence, & substitution effects affecting incentives for security investment. *Journal of Accounting and Public Policy*, 25(6), 629–665.

Homer, J., & Oliva, R. (2001). Maps and models in system dynamics: A response to Coyle. *System Dynamics Review*, *17*(4), 347–355. http://doi.org/10.1002/sdr.224

Hoo, K. J. S. (2000). *How Much Is Enough ? A Risk-Management Approach to Computer Security*. Palo Alto.

Howard, M., & LeBlanc, D. (2002). *Writing Secure Code* (Second ed.). Seattle, WA: Microsoft Press.

Huang, C.D. (2010). Optimal Investment in Information Security: A Business Value Approach. *PACIS 2010 Proceedings*.

Huang, C.D., Hu, Q., & Behara, R.S. (2006). Economics of information security investment in the case of simultaneous attacks. *The Fifth Workshop on the Economics of Information Security*. URI: http://weis2006.econinfosec.org/docs/15.pdf

Huang, C. D., Behara, R.S., & Hu, Q. (2007). Economics of information security investment. In *Handbooks in Information Systems*, 53–69.

Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *Int. J. Production Economics, 114*, 793–804. http://doi.org/10.1016/j.ijpe.2008.04.002

Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics*, 141 (1), 255-268.

Huang, C. D., & Goo, J. (2009). Investment Decision on Information System Security: A Scenario Approach. In *Proceedings of AMCIS 2009*.

Jonsson, E., & Olovsson, T. (1997). A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior. *IEEE Transactions on Software Engineering*, 23(4), 235-245.

Kiely, L., & Benzel, T. V. (2006). Systemic security management. *IEEE security & privacy*, *4*(6).

Kort, P.M., Haunschmied, J.L., & Feichtinger, G. (1999). Optimal firm investment in security. *Annals of Operations Research,* 88(0), 81–98.

Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, *38*(2), 451–471.

Lane, D.C. (1999). Social Theory and System Dynamics Practice. *European Journal of Operational Research*, *113*, 501–527.

LeCompte, M. & Preissle, J. (1993). *Ethnography and qualitative design in educational research (2nd ed.).* San Diego, CA: Academic Press.

Lee, Y.J., Kauffman, R.J., & Sougstad, R. (2011). Profit-maximizing firm investments in customer information security. *Decision Support Systems,* 51(4), 904–920.

Leeson, P.T., & Coyne, C.J. (2006). The Economics of Computer Hacking. *Journal of Law, Economics and Policy,* forthcoming.

Liu, D., Ji, Y., & Mookerjee, V. (2005). Information Security Investment with Different Information Types: A Two- Firm Analysis. *AMCIS 2005 Proceedings.*

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems,* 52(1), 95–107.

Luna-Reyes, L. F., & Andersen, D. L. (2003). Collecting and analyzing qualitative data for system dynamics: Methods and models. *System Dynamics Review*, *19*(4), 271–296.

Martinez-Moyano, I. J., Conrad, S. H., & Andersen, D. F. (2011). Modeling behavioral considerations related to information security. *Computers and Security*, *30*(6–7), 397–409.

Martinez-Moyano, I. J., Oliva, R., Morrison, D., & Sallach, D. (2015). Modeling Adversarial Dynamics. In *Proceedings of the 2015 Winter Simulation Conference*, 2412–2423.

McAfee. (2014). *Net losses: Estimating the global cost of cybercrime: Economic impact of cybercrime II* (June). Available at: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf).

McKay, M., Conover, W., & Beckman, R. (1979). A comparison of three methods for selecting values of input variables in the analysis of output from a computer code. *Technometrics,* 21, 339-45

Microsoft. (2014). Microsoft Enterprise Cloud Red Teaming. *Microsoft,* 9-14.

Mizzi, A. (2010). Return on information security investment-the viability of an anti-spam solution in a wireless environment. *International Journal of Network Security,* 10(1), 18–24.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management*, *52*(1), 123–134.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Sprouts: Working Papers on Information Systems*, 10(26), 1-51.

Pindyck, R. (1991). Irreversibility, Uncertainty and Investment. *Journal of Economic Literature*, *XXIX*(September), 1110–1148.

Purser, S.A. (2004). Improving the ROI of the security management process. *Computers & Security* 23(7), 542–546.

Repenning, N. (2002). A simulation-based approach to understanding the dynamics of innovation implementation. *Organization Science*, *13*(2), 109–127.

Richardson, G. (2013). Concept Models in Group Model Building. *System Dynamics Review*, *29*(1), 42–55. http://doi.org/10.1002/sdr

Richardson G., & Pugh, A.L, III. (1981). Introduction to System Dynamics Modeling with DYNAMO. *MIT Press*. Cambridge, MA.

Shim, W. (2011). Vulnerability & Information Security Investment Under Interdependent Risks: A Theoretical Approach. *Asia Pacific Journal of Information Systems*, 21(4), 2743.

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)-A practical quantitative model. *Journal of Research and Practice in Information Technology*, 38(1), 45–56.

Sterman, J. (2000). *Business Dynamics. Systems Thinking and Modeling for a Complex World*. Boston: McGraw Hill Higher Education.

Stewart, M. J. (2014). *Network Security, Firewalls, and VPNs* (Second ed.). London: Jones & Bartlett Learning.

Suby, M., & Dickson, F. (2015). The 2015 (ISC) Global Information Security Workforce Study. *A Frost & Sullivan White Paper*, 1–28. Retrieved from https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)?-Global-Information-Security-Workforce-Study-2015.pdf

Sun, H. (2013). A longitudinal study of herd behavior in the adoption and continued use of technology. *MIS Quarterly*, 37(4), 1013–1041.

Sun, W., Kong, X., He, D., & You, X. (2008). Information Security Problem Research Based on Game Theory. In *International Symposium on Electronic Commerce and Security*, 554–557.

Tipton, H. & Krause, M. (2006). *Information Security Management Handbook. Fifth Edition, Volume 3* (5th ed.). Auerbach Publications, Boston, MA, USA

Varian, H., (2002). System Reliability and Free Riding, *Workshop on the Economics of Information Security*, May, 16–17, Berkeley, CA.

Varian, H. (2004). System reliability and free riding. *Economics of Information Security*, (February), 1–15. http://doi.org/10.1007/1-4020-8090-5_1

Vennix, J. A. M. (1996). *Group model building: Facilitating team learning using system dynamics.* Chichester, UK: Wiley.

Verizon (2016). *2016 Data Breach Investigations Report.* Basking Ridge, NY. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Wang, S.L., Chen, J.D., Stirpe, P.A., & Hong, T.P. (2009). Risk-neutral evaluation of information security investment on data centers. *Journal of Intelligent Information Systems,* 36(3), 329–345.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2), 13-23.

Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, *46*(8), 91–95. http://doi.org/10.1145/859670.859675

Willemson, J. (2006). On the Gordon & Loeb model for information security investment. *The Fifth Workshop on the Economics of Information Security*, University of Cambridge, England.

Willemson, J. (2010). Extending the Gordon and Loeb Model for Information Security Investment. In *Proceedings of International Conference on Availability, Reliability, and Security,* 258–261.

Wolstenholme, E.F., Coyle, R.G. (1983). The development of system dynamics as a rigorous procedure for system description. *Journal of the Operational Research Society,* 34, 569-581.

References from Newspapers, Magazines, Blogs and Webpages:

Anderson, R., & Schneier, B. (2005). Economics of Information Security. *IEEE Security & Privacy*, *Jan/Feb*, 24–25. Retrieved from https://www.schneier.com/academic/paperfiles/paper-economics.pdf

eWEEK. 2016. “Spending on Information Security Expected to rise in 2016,”, January (available at http://www.eweek.com/it-management/spending-on-information-security-expected-to-rise-in-2016.html).

Gartner. 2016. “Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to reach$81.6 Billion in 2016,”, August (available at http://www.gartner.com/newsroom/id/3404817).

Graham, C. (2017, May 13). "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history. *The Daily Telegraph*. Retrieved from http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

Gordon, L. A., & Richardson, R. (2004, April 13). The New Economics of Information Security. *Information Week*, 53-56. Retrieved from http://www.banktech.com/management-strategies/the-new-economics-of-information-security-/d/d-id/1289804?

Hern, A., & Gibbs, S. (2017, May 12). "What is 'WanaCrypt0r 2.0' ransomware and why is it attacking the NHS? *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20

Kroustek, J. (2017, May 12). "Avast reports on WanaCrypt0r 2.0 ransomware that infected NHS and Telefonica". Avast Security News. Avast Software Inc. Retrieved from https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today

The Guardian. 2010. "WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback,", December (available at http://www.theguardian.com/world/2010/dec/08/wikileaks-visamastercard-operation-payback).

The Guardian. 2016. "Yahoo hack: 1bn accounts compromised by biggest data breach in history,", December (available at https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached).

The Washington Post. 2014. "The Sony Pictures hack, explained,", December (available at http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/the-sony-pictureshackexplained/).

Appendix

List of Equations

SD Symbol	Name	Unit	Definition
Converter	# of Dismissed Attacks	Attacks	3<<Attacks>>
Stock	Accumulated Attackers Wealth	Euros	0
Flow	Accumulated Attackers Wealth.Increasing Attacker Weatlh.in		'Increasing Attacker Weatlh'
Stock	Accumulated Successful Attacks Vector A	Attacks	10
Flow	Accumulated Successful Attacks Vector A.Breaches Vector A.in		'Breaches Vector A'
Stock	Accumulated Successful Attacks Vector B	Attacks	7
Flow	Accumulated Successful Attacks Vector B.Breaches Vector B.in		'Breaches Vector B'
Stock	Accumulated Successful Attacks Vector C	Attacks	5
Flow	Accumulated Successful Attacks Vector C.Breaches Vector C.in		'Breaches Vector C'
Constant	Activate Uncertainty	Dimensionless	0
Converter	Adjustment	Reppoints	'Indicated Reputation'-Reputation
Converter	Attack Unitary Cost	Euros/Attacks	10<<Euros/Attacks>>
Converter	Attackers Capabilities	Attacks	100<<Attacks>>
Converter	Attackers Performance	Euros/Month	(('Breaches Vector A')+('Breaches Vector B')+('Breaches Vector C'))*'Attack Unitary Cost'
Converter	Base financial performance	Euros	50
Constant	Base reputation	Reppoints	100
Flow	Breaches Vector A	Attacks/Month	'Successful Attacks Vector A'/'Time to report attack'
Flow	Breaches Vector B	Attacks/Month	'Successful Attacks Vector B'/'Time to report attack'
Flow	Breaches Vector C	Attacks/Month	'Successful Attacks Vector C'/'Time to report attack'
Flow	Building Up	Reppoints/Month	IF(Adjustment>0<<Reppoints>>,(Adjustment/'Time to build up reputation'),0<<Reppoints/Month>>)

Stock	Defenders Accumulated Profits	Euros	0
Flow	Defenders Accumulated Profits.Increasing Financial Performance.in		'Increasing Financial Performance'
Converter	Defenders Capabilities	Euros	1000<<Euros>>
Converter	Defenders Financial Performance	Euros/Month	('Reputation to money rate'*Reputation)+'Base financial performance'
Constant	Dismissal time	Month	1
Flow	Dismissed A	Attacks/Month	'# of Dismissed Attacks'/'Dismissal time'
Flow	Dismissed B	Attacks/Month	'# of Dismissed Attacks'/'Dismissal time'
Flow	Dismissed C	Attacks/Month	'# of Dismissed Attacks'/'Dismissal time'
Flow	Erosion	Reppoints/Month	IF(Adjustment<0<<Reppoints>>,(ABS(Adjustment/'Time reputation loss')),0<<Reppoints/Month>>)
Converter	Fraction Investment Vector A	Dimensionless	'Reported Successful Attacks Vector A'/('Reported Successful Attacks Vector A'+'Reported Successful Attacks Vector B'+'Reported Successful Attacks Vector C')
Converter	Fraction Investment Vector B	Dimensionless	'Reported Successful Attacks Vector B'/('Reported Successful Attacks Vector A'+'Reported Successful Attacks Vector B'+'Reported Successful Attacks Vector C')
Converter	Fraction Investment Vector C	Dimensionless	'Reported Successful Attacks Vector C'/('Reported Successful Attacks Vector A'+'Reported Successful Attacks Vector B'+'Reported Successful Attacks Vector C')
Converter	Fraction of Attack Vector A	Dimensionless	'Switch A'*'Accumulated Successful Attacks Vector A'/('Accumulated Successful Attacks Vector A'+'Switch B'*'Accumulated Successful Attacks Vector B'+'Switch C'*'Accumulated Successful Attacks Vector C')
Converter	Fraction of Attack Vector B	Dimensionless	'Switch B'*'Accumulated Successful Attacks Vector B'/('Switch A'*'Accumulated Successful Attacks Vector A'+'Accumulated Successful Attacks Vector B'+'Switch C'*'Accumulated Successful Attacks Vector C')
Converter	Fraction of Attack Vector C	Dimensionless	'Switch C'*'Accumulated Successful Attacks Vector C'/('Switch A'*'Accumulated Successful Attacks Vector A'+'Switch B'*'Accumulated Successful Attacks Vector B'+'Accumulated Successful Attacks Vector C')
Converter	High UNC	Dimensionless	'Information Sharing'*RANDOM(MIN((0.75+0.00498*TIME),0.999),MAX(1.5-(0.00998)*TIME,1.001))+(1-'Information Sharing')*RANDOM(0.75,1.5)
Flow	Increasing Attacker Weatlh	Euros/Month	'Attackers Performance'

Flow	Increasing Financial Performance	Euros/Month	'Defenders Financial Performance'
Converter	Indicated Reputation	Reppoints	'Base reputation'-('Vector A Value'*'Vulnerability Vector A')-('Vector B Value'*'Vulnerability Vector B')-('Vector C Value'*'Vulnerability Vector C')
Constant	Information Sharing	Dimensionless	0
Converter	Low UNC	Dimensionless	'Information Sharing'*RANDOM(MIN((0.95+0.0008*TIME),0.999),MAX(1.1-(0.0018)*TIME,1.001))+(1-'Information Sharing')*RANDOM(0.95,1.1)
Converter	Medium UNC	Dimensionless	'Information Sharing'*RANDOM(MIN((0.875+0.00248*TIME),0.999),MAX(1.25-(0.00498)*TIME,1.001))+(1-'Information Sharing')*RANDOM(0.875,1.25)
Converter	Past value A	Attacks	DELAYPPL('Accumulated Successful Attacks Vector A',1,0<<Attacks>>)
Converter	Past value B	Attacks	DELAYPPL('Accumulated Successful Attacks Vector B',1,0<<Attacks>>)
Converter	Past value C	Attacks	DELAYPPL('Accumulated Successful Attacks Vector C',1,0<<Attacks>>)
Stock	Reported Successful Attacks Vector A	Attacks	5
Flow	Reported Successful Attacks Vector A.Dismissed A.out		'Dismissed A'
Flow	Reported Successful Attacks Vector A.Reports Vector A.in		'Reports Vector A'
Stock	Reported Successful Attacks Vector B	Attacks	5
Flow	Reported Successful Attacks Vector B.Dismissed B.out		'Dismissed B'
Flow	Reported Successful Attacks Vector B.Reports Vector B.in		'Reports Vector B'
Stock	Reported Successful Attacks Vector C	Attacks	5
Flow	Reported Successful Attacks Vector C.Dismissed C.out		'Dismissed C'
Flow	Reported Successful Attacks Vector C.Reports Vector C.in		'Reports Vector C'
Flow	Reports Vector C	Attacks/Month	'Successful Attacks Vector C'/'Time to report attack'
Flow	Reports Vector A	Attacks/Month	'Successful Attacks Vector A'/'Time to report attack'
Flow	Reports Vector B	Attacks/Month	'Successful Attacks Vector B'/'Time to report attack'
Stock	Reputation	Reppoints	50

Flow	Reputation.Building Up.in		'Building Up'
Flow	Reputation.Erosion.out		Erosion
Converter	Reputation to money rate	Euros/(Reppoints*Month)	10
Converter	Successful Attacks Vector A	Attacks	IF('Vulnerability Vector A'>0<<Euros>>,(('Attackers Capabilities'*'Fraction of Attack Vector A')-(('Defenders Capabilities'*'Fraction Investment Vector A')/'Attack Unitary Cost')),0<<Attacks>>)
Converter	Successful Attacks Vector B	Attacks	IF('Vulnerability Vector B'>0<<Euros>>,(('Attackers Capabilities'*'Fraction of Attack Vector B')-(('Defenders Capabilities'*'Fraction Investment Vector B')/'Attack Unitary Cost')),0<<Attacks>>)
Converter	Successful Attacks Vector C	Attacks	IF('Vulnerability Vector C'>0<<Euros>>,(('Attackers Capabilities'*'Fraction of Attack Vector C')-(('Defenders Capabilities'*'Fraction Investment Vector C')/'Attack Unitary Cost')),0<<Attacks>>)
Converter	Switch A	Dimensionless	IF('Accumulated Successful Attacks Vector A'-'Past value A'<1<<Attacks>>,0,1)
Converter	Switch B	Dimensionless	IF('Accumulated Successful Attacks Vector B'-'Past value B'<1<<Attacks>>,0,1)
Converter	Switch C	Dimensionless	IF('Accumulated Successful Attacks Vector C'-'Past value C'<1<<Attacks>>,0,1)
Constant	Time reputation loss	Month	1
Constant	Time to build up reputation	Month	6
Constant	Time to report attack	Month	1
Converter	Uncertainty	Dimensionless	IF('Activate Uncertainty'=0,1,IF('Activate Uncertainty'=2,'Medium UNC',IF('Activate Uncertainty'=1,'Low UNC','High UNC')))
Converter	Vector A Value	Reppoints/Euros	1
Converter	Vector B Value	Reppoints/Euros	1
Converter	Vector C Value	Reppoints/Euros	1
Converter	Vulnerability Vector A	Euros	('Attackers Capabilities'*'Fraction of Attack Vector A'*'Attack Unitary Cost'*Uncertainty)-('Defenders Capabilities'*'Fraction Investment Vector A')
Converter	Vulnerability Vector B	Euros	('Attackers Capabilities'*'Fraction of Attack Vector B'*'Attack Unitary Cost'*Uncertainty)-('Defenders Capabilities'*'Fraction Investment Vector B')
Converter	Vulnerability Vector C	Euros	('Attackers Capabilities'*'Fraction of Attack Vector C'*'Attack Unitary Cost'*Uncertainty)-('Defenders Capabilities'*'Fraction Investment Vector C')