Analysing the impact of cyber insurance on the cyber security ecosystem

Utilising agent-based modelling to explore the effects of insurance policies

TU Delft

This page is intentionally left blank

Analysing the impact of cyber insurance on the cyber security ecosystem

Utilising agent-based modelling to explore the effects of insurance policies

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in Complex Systems Engineering and Management

Faculty of Technology, Policy and Management

By

Jhoties Sewnandan

Student number: 4330188

To be defended in public on October 15th, 2018

Graduation committee

Chairperson :	Prof. dr. ir. M. J. G. van Eeten, Organisation & Governance
First Supervisor :	Dr.ir. W. Pieters, Safety and Security Science
Second Supervisor :	Dr.ir. E.J.L. Chappin, Energy and Industry

This page is intentionally left blank

Preface

Throughout my studies I have always sought something that I found interesting, exciting and really worth doing. However, it wasn't until I did the course agent-based modelling that I thought this is it. Therefore, it was only logical that I chose a thesis project which allowed me to utilise the skills I cultivated throughout my master to create and use an agent-based model. To my surprise I was able to find a thesis project that related to agent-based modelling and to another of my interests, cyber security, at the graduation market of our faculty. As such, the subject of analysing the influence of cyber insurance on the cyber security ecosystem was an opportunity I couldn't pass up.

This thesis was written as the graduation project for the master 'Complex Systems Engineering and Management' of the TU Delft. The thesis contains research towards cyber insurance policies which is one of the subjects which has had very little coverage in literature. In this graduation project an attempt has been made to close the knowledge gap on this subject by analysing the influence that cyber insurance has on the ecosystem based on the insurance policies that are used. As such, the thesis was written for those that want to gain more knowledge on what it means to have cyber insurance as an option to mitigate risk on an ecosystem level and for those that want to understand the effects of several cyber insurance policies on the ecosystem.

This page is intentionally left blank

Acknowledgements

This graduation project marks the end of my academic career at the TU Delft. This university and specifically the faculty of technology, policy and management have always motivated me to improve and become more skilled which is a mind-set that will be of great use to me in my professional career as well. However, I would have never been able to achieve what I have by myself. Therefore, I would like to express gratitude for those that have helped and supported me to make all of this possible.

First, I would like to express gratitude to my committee, Wolter Pieters, Emile Chappin and Michel van Eeten for the feedback and discussions on my work. Their comments on the scope, model decisions and results have helped me a great deal in improving the quality of my work. Furthermore, I would like to specifically thank Wolter Pieters for being my first supervisor and guiding me throughout the writing and structuring of my graduation project. His critical assessments made me reflect on my project several times which allowed me to stay focussed and improve clarity in the report.

Second, I would like to thank the fellow students that I convened with for study sessions. They have helped me a lot in tackling the structuring issues I faced for my report and in issues I faced in modelling the cyber security ecosystem. Thanks to them I was able to stay on track and finish the research I set out to do.

Last but not least, I would like to thank my family for the support they have given me throughout my studies. Without their support I would have been unable to achieve anything. They have motivated me to never give up and have made it possible for me to give it my all in my academic career.

Jhoties Sewnandan

Amsterdam, October 2018

This page is intentionally left blank

Executive summary

One of the largest issues for organisations is to protect themselves from the malicious intentions of cyber attackers. This can be difficult to do for several reasons, for example, there are many different controls available and the effectiveness of controls cannot be measured. Additionally, there is also uncertainty surrounding the process. To this end, insurance firms have stepped into the cyber security ecosystem, selling risk displacement as their product. However, the ecosystem has shown a lack of adoption of cyber insurance. This has interested researchers and has led to much literature on how cyber insurance can be beneficial and what effects it has. However, the current literature is missing one vital element, the dynamic nature of the cyber security ecosystem, which is defined by the chaos, interconnectivity and unpredictability in the system. Without the taking the dynamic nature in account, the effects and potential of cyber insurance cannot be fully understood. Furthermore, research towards insurance policies and how these can be used to influence the system has had very little attention in literature, whilst it can provide valuable insight into the effects of cyber insurance.

This thesis has focussed on capturing the dynamicity of the system, providing clarity into the effects of cyber insurance and gaining insight on the policies that insurance firms can use to influence the ecosystem. The main research question that was answered in this thesis was:

How do various cyber insurance policies affect the total damage in the cyber security ecosystem over time?

The research objectives in this thesis consisted of four parts. First the cyber security ecosystem had to be identified and decomposed in order to make modelling possible. The second research objective concerned itself with understanding insurance firms and the policies they can employ to influence the system. The third research objective was focussed on bringing the model and the information on insurance policies together in order to create an experimental design. The final research objective was aimed at performing the experiment that was designed and analysing the data in order to understand the effects of the insurance policy options. Furthermore, the goal was to use the insight obtained to identify synergies and design a new insurance policy aimed at bringing forth a positive effect on the entire ecosystem.

In order to fulfil these research objectives and provide an answer to the main question, agent-based modelling has been utilised. Agent-based modelling makes it possible to simulate complex and dynamic systems like the cyber security ecosystem. Furthermore, the agent-based models are very well suited for exploration and experimentation.

The research is focussed on the cyber security ecosystem. Therefore, the main concepts relate to the behaviour and interactions of the actors within this system. Based on the main interactions of the actors a conceptual model was created, the conceptual model is shown in figure 1.

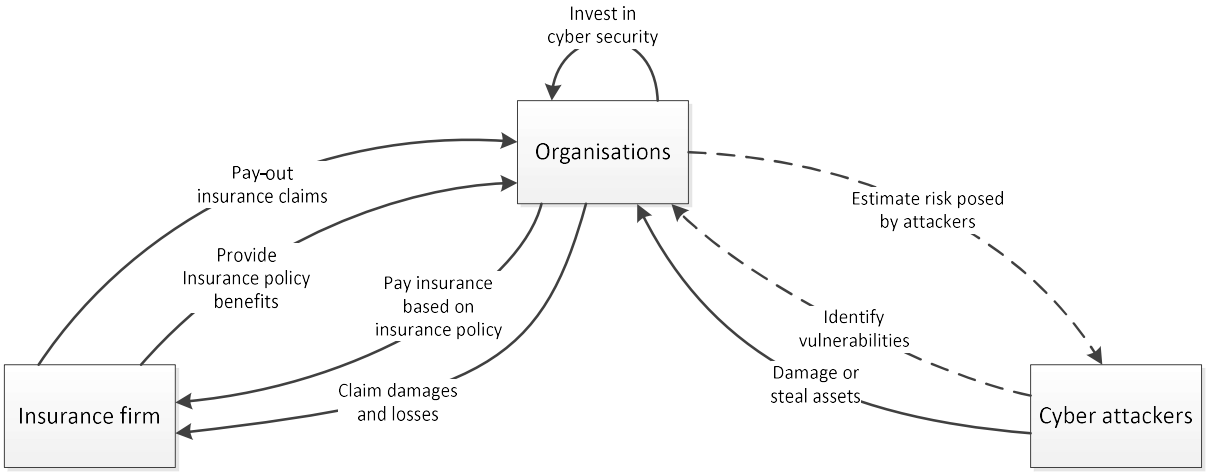

Figure 1: Conceptual model of the cyber ecosystem

Three actors were identified: organisations, attackers and insurance firms. Organisations defend themselves from attackers by conducting a cyber risk management process. During this process organisations assess their risk and determine what they will do in order to reduce it. Cyber insurance is one of the possible options and is considered based on the insurance policy of the insurance firm. A contract will be made if the conditions of the policy are acceptable and remaining budget will be invested to reduce remaining risk if necessary. There are several options that an insurance firm can add to their insurance policy to influence the behaviour of the organisation. Seven of these policy options were identified through literature and were used for experimentation on the ecosystem: insurance package (premium and coverage combination), contract length, risk selection, incentivisation, upfront risk assessment, sharing cyber security control information and requiring organisations to maintain their security level.

The agent-based model was built based on these concepts and simulates the behaviour and interactions of the actors. Through parametrisation and by measuring the output of each run, the model was made useful for exploring and experimenting with the effects of different parameter values providing insight into the effects these would have on the ecosystem.

The experimental design that was created to test the influence of various insurance policies setups on the ecosystem was made up of the seven insurance policy options mentioned above. The policy option parameters along with baseline values for other parameters formed the experimental design. A choice was made to perform a full factorial experiment because this made it possible to design new policies based on possible synergies between insurance policy options.

The main findings indicated that the influence of the cyber insurance policies were quite small on the global metrics but did show positive results. These small effects could mainly be attributed to a low number of organisations that were insured in most cases since this reduces the observable effect on the global metrics. However, a new policy was also designed comprised of a contract length, required security level, incentivisation and sharing insurance data. The designed experiment results showed that there were some synergy effects in play as well. The effect of an insurance policy was quite clear when looking at insured organisation metrics. However, when looking at the global metrics, the values ended up becoming rather low again. One main takeaway from the experiment is that insurance has a negative influence on the cyber security ecosystem by default. This is because cyber insurance displaces risk but costs money without increasing cyber security strength. This means that

organisations have fewer budgets available for investments and thus have a lower cyber security level compared to uninsured organisations. Therefore, insured organisation end up incurring more losses compared to uninsured organisations. This is an effect that insurance policies would have to overcome before insurance can be a positive influence on the whole ecosystem. However, do take note that the losses mentioned refer to the total value that attackers steal and thus does not have to reflect the welfare of an organisation since they can claim those losses. An organisation can still be better off financially by buying insurance instead of continually investing into cyber security.

Two main contributions were made in this thesis. First the influence and synergy of various cyber insurance options have been clarified to an extent. The experiment performed in this thesis has tested the effects of various cyber insurance policies in order to see how these can influence the cyber security ecosystem. This also goes beyond the academic literature since the results from this thesis are on ecosystem level and have been generated through a dynamic model. The second contribution is the model itself. In literature, an agent-based model has not been used before to simulate the effect of cyber insurance. Furthermore, the model itself provides a lot of possibilities for expansion and customisation which could be invaluable to future research. The cyber security ecosystem is also a chaotic system by nature which makes using dynamic models more useful for obtaining insights compared to the methods used in current literature.

There are several limitations and assumptions that impact the interpretability of the results and insights. First, the ecosystem had to be abstracted before it could be modelled which can cause important mechanisms to get lost or simplified. Another limitation is that no real data could be used as input for the model. Instead the model was validated through the concepts and mechanisms it was built upon. Furthermore, the model was built, using several simplifying assumptions. The assumptions were made to reduce complexity but can influence the behaviour of the model and thus the results of the experiments. For example, the organisations in the model only possess assets value, which reflects the total financial value of all their assets. Whilst, in the actual ecosystem, organisations can consider an asset invaluable which might not be recoverable when breached, for instance the corporate image of an organisation. This would influence the choice to obtain insurance or not.

Table of contents

1. Introduction

In 2016, worldwide $81.6 billion was invested in cyber security (Gartner, 2016). This remains an important field for organisations to invest in as part of their cyber risk management, since being breached can have devastating effects for them (loss of money, leak of customer information, negative publicity, et cetera). As an alternative to risk reduction through controls (cyber security), cyber insurance was introduced, this gave organisations the choice to: invest their budget into cyber security and/or buy cyber insurance.

Cyber insurance has influenced the ecosystem of cyber attackers and defenders since it has provided defenders with a new option to invest in. However, it is still not exactly clear in how cyber insurance specifically affects the ecosystem. One particular question surrounding cyber insurance is whether buying cyber insurance causes investment problems for organisations (Gordon, Loeb, & Sohail, 2003; Pal & Golubchik, 2010; Zhao, Xue, & Whinston, 2013). This question is raised since investment problems would show itself in the form of reduced cyber security leading to more losses through cyberattacks. Furthermore, a moral hazard could come into play which means that the organisations purposely stop investing once the risk becomes acceptable and thus save money.

In the field of cyber risk management different opinions have been expressed on the effects of cyber insurance. Several researchers state that cyber insurance is beneficial to the overall security against cyberattacks (Bolot & Lelarge, 2009; Yang & Lui, 2014), whilst others suggest that cyber insurance has no effect at all or even a negative effect on cyber security of organisations (Pal, Golubchik, Psounis, & Hui, 2014; Shetty, Schwartz, Felegyhazi, & Walrand, 2010). The former suggesting that there is no or an insignificant investment problem allowing cyber insurance to be beneficial to organisations, whilst the latter suggests that an investment problem does occur. Furthermore, the market for cyber insurance has not grown as fast as expected, a conservative forecast in 2002 predicted a market worth of $2.5 billion in 2005 which has not been reached until 2015 where the value was $2.75 billion (Betterly, 2015; Böhme, Schwartz, & others, 2010). The slow growth is a possible indication of problems which caused organisations to opt for investments in controls instead. Whether this can be contributed to investment problems, distrust in cyber insurance or because cyber insurance was just not appealing enough is not clear. However, Betterly (2015) also states that the market has started growing with half of the insurance firms stating a growth between 26-50% in 2015. This more recent increase can indicate that the cyber insurance market is becoming more appealing to organisations. The opinions expressed in literature and growth of the market become more understandable when taking a closer look at cyber insurance and the role it plays in the ecosystem.

1.1 Cyber risk management in general

The cyber security ecosystem is based around two actors, organisations and attackers. There are organisations conducting business all around the world. By doing so, organisations tend to amass great amounts of value in the form of assets which allows them to compete with their competitors and keep growing on the market. However, because they amass such wealth in assets, they become targets for attackers that desire to obtain it. Furthermore, the increasing use and integration of ICT in organisations makes them especially vulnerable for cyberattacks as well. Furthermore, cyberattacks are relatively cheap to conduct and are virtually untraceable. Thus attackers can keep attacking without actually being caught (Marotta, Martinelli, Nanni, Orlando, & Yautsiukhin, 2017). The risk of cyberattacks occurring has caused organisations to take various measures to prevent being breached

and losing assets. This has led to the rise of cyber risk management processes, through which organisations assess their risk and vulnerabilities and attempt to take appropriate measures to reduce their risk. Cyber insurance firms are added into the system as a third actor that presents organisations with a different way to reduce their risk. Insurance firms will take on the risk of organisations against specific premiums and will pay-out according to the insurance policy when they are breached.

1.2 Role of cyber insurance

Cyber insurance can be useful to organisations as it helps them to displace risk and financially regain losses at a fixed cost. However, financial losses aren't the only damage an organisation incurs as a result of cyberattacks. Jones et al. (2005) names four types of loss: asset loss, threat loss, organisational loss and external loss. The different types of losses have proven to be difficult to quantify financially and can be differently valued by organisations as well. This causes insurance firms to usually not insure the entire (perceived) value that is lost in a cyberattack (Marotta et al., 2017). Moreover, a premium has to be paid to obtain cyber insurance which leaves fewer budgets available for investment in controls. This is one of the reasons why cyber insurance can be less appealing to organisations and causes them to prefer investing in their own cyber security (controls) to protect their assets instead of relying on cyber insurance. However, because insurance firms work with several organisations they also gain experience and knowledge which can be used to advice and help organisations make better investment choices. This would create a positive effect on the cyber security in the market but it is unclear if, for instance, moral hazard would undo this effect.

Insurance firms make use of premiums and policies in which they state what damages they will insure and to what end the insurance is provided (Böhme et al., 2010; Gordon et al., 2003; ulisi Ogut & Raghunathan, 2005). For example, insurance will cover only intellectual property loss and not image loss, or insurance will only be provided when the organisation invests a certain amount in cyber security annually. Additionally, limits to the pay-out can also be used i.e. coverage up to €200.000 for certain types of loss. However, whilst these policies are used by insurers to manage the risk of insuring organisations, they can also become a driving force to increase cyber security (Pal & Golubchik, 2010). Understanding the effects of cyber insurance policies and whether it causes investment or other problems, can therefore also lead to design of insurance policies that can drive organisations to continue improving their cyber security.

1.3 Knowledge gap

In the current literature on the cyber security ecosystem, various researches have been done on the effect of cyber insurance. Researchers have hypothesised over the effects of cyber insurance and used various methods to test it. Under known literature, research has been done towards the role cyber insurance plays in the cyber risk management of organisations and on the effects of cyber insurance on networks of organisations. Whilst the current literature is very useful to the understanding of cyber insurance and provides insight into some of the effects, it still falls short in several ways.

Current literature tends to mostly focus on the direct effects of cyber insurance, not taking into account the indirect effects it could have. For instance, quite some research was done on how cyber insurance can be part of the cyber risk management strategy of organisations (Böhme, 2010; Gordon et al., 2003). In these papers research is done into how cyber insurance can displace risk and how it

can be beneficial to the reduction of cyber risk. However, these papers do not consider the indirect effects, for instance how will it affect the cyber security level of the organisation and will it lead to the organisation being attacked more often. These indirect effects are still unclear, thus the effects of cyber insurance on the ecosystem are unclear.

From the literature that did focus on the effects that cyber insurance brings forth, most of the studies have made use of conceptual and mathematical models to analyse the system (Pal & Golubchik, 2010; Pal et al., 2014; Yang & Lui, 2014). These models are useful to understand various aspects of cyber insurance and its effects. However, the downside of these kinds of models is that they lack the dynamicity and interaction between entities and components. This is a critical aspect for the cyber security ecosystem since there is a lot of uncertainty and irregularity in the system. For instance, there are no standards that can help in the assessment of cyber security and risk which is something organisations struggle with when deciding on their investments. Another example concerns attacks, these can be very difficult to define since there are many types of attackers and tools and they occur irregularly. Therefore, in order to gain more valuable insights into the effects of cyber insurance, the dynamicity of the system should be taken into account.

In literature there has also been a tendency to focus on a single entity, where the research is aimed towards gaining an understanding for that specific entity. For instance wanting to know how insurance firms grow in the market (Bandyopadhyay, Mookerjee, & Rao, 2009) or looking from the perspective of risk reduction in organisations (Zhao et al., 2013). These researches provide some insight into the effects of cyber insurance from one perspective. However, as was mentioned above, the interactions between entities and components are a vital part of the cyber security ecosystem. Therefore, when looking at the whole system, the effects of cyber insurance might end up being different compared to the results from the papers.

Literature also does not address the synergies that could be achieved through the usage of various cyber insurance policies. This is likely attributed to there being very little research into the policies that insurance firms can use.

By analysing the system in its entirety and addressing the dynamics in the system more insight can be obtained on how cyber insurance and its insurance policies influence the ecosystem. Moreover, this can show how cyber insurance can become a driving force for cyber security investments in organisations as to minimise losses.

1.4 Proposed research

In order to overcome the knowledge gap and provide more clarity, a modelling approach using ABM (Agent-Based Modelling) has been selected to simulate the system and test the effects of cyber insurance on the ecosystem. Modelling was chosen as research approach since modelling makes it possible to simulate and analyse dynamic systems such as cyber risk management and to analyse the interconnectedness in a system. ABM was selected as modelling tool since this tool makes it possible to create complex decision making processes and model interactions between agents (Novak, Kadera, & Wimmer, 2017). Therefore, it is a good fit as the aim is to research the emergent behaviour in the ecosystem brought forth by the policies used by insurance firms in the system. The structure of ABM models also lend itself for experimentation thus allowing for design and analysis of various insurance policies.

In this research the system of attackers and defenders will be simulated in order to study the effect cyber insurance has on organisations. Where the focus will be set on analysing the impact various cyber insurance policies have on cyber security investments of organisations and the attacks / value loss that organisations suffer as a result.
Therefore, the research question is:

How do various cyber insurance policies affect the total damage in the cyber security ecosystem over time?

As mentioned before, ABM will be used to simulate the system to capture the dynamicity. The insurance ecosystem has many stakeholders which make the system complex to model. Therefore, the thesis is scoped to include the insurance firms, organisations and attackers along with their interactions. A conceptual model for this scope was created based on literature and the cyber insurance ecosystem model by Labunets et al. (2018) and is shown in figure 1-1. This scope will make it possible to perform the research within the CoSEM thesis limitations. The use of the ABM model will provide insight into the effect of cyber insurance on the investments of organisations and also on the long term losses of organisations. Furthermore, in the model various insurance policies will be experimented with to see how different policies effect organisations.

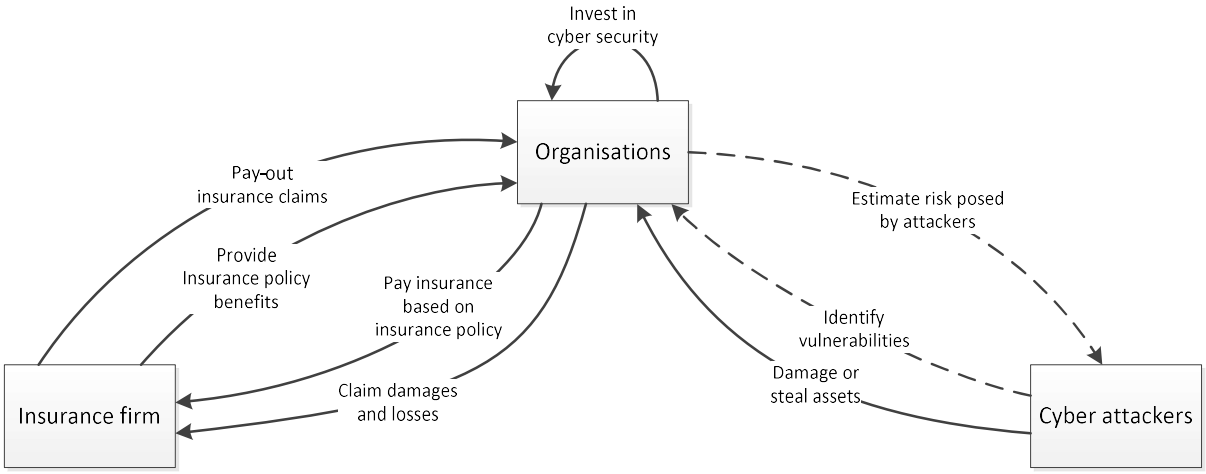

Figure 1-1: Conceptual model of the cyber ecosystem according to thesis scope

Research objectives
Four research objectives have been formulated in order to answer the research question.

1. Identify the cyber security ecosystem and the behaviours and interactions of the actors in it to facilitate the creation of a simulation model
2. Determine and understand the cyber insurance policies that can be used by insurance firms to influence the ecosystem
3. Create an experimental design through the use of the simulation model and knowledge gathered on insurance policies
4. Perform the experiment using the experimental design, analyse the results and design a new insurance policy has a positive influence on the cyber security ecosystem.

The first research objective is to identify and decompose the cyber security ecosystem in order to make modelling possible. The second research objective is aimed at understanding insurance firms

and the policies they can employ to influence the system. The third research objective is focussed on bringing the model and the information on insurance policies together in order to create an experimental design. The final research objective is aimed at performing the experiment that was designed and analysing the data in order to understand the effects of the insurance policy options. Additionally, a new insurance policy will be designed based on possible synergies and its effects on the ecosystem will be analysed.

Sub questions

Based on the research objectives, four sub questions have been formulated. The answers to these sub-questions will serve as input for the ABM model and will also provide information for answering the research question. Sub questions 1 and 2 are aimed at understanding the actors in the system up to the level necessary to conceptualise the ABM model. As such these two sub questions will identify the concepts necessary to model the ecosystem. Sub questions 3 and 4 will be answered through use of the ABM model. The sub questions are discussed below.

The first sub question is the following:

1. *What behaviour and decision making mechanisms are part of each actor in the cyber security ecosystem and how do these actors interact with each other?*

This sub question is focussed on determining the behaviour and interactions of organisations, attackers and insurance firms. Furthermore, for each of these actors, the decision making mechanisms will be identified to facilitate modelling of these actors.

For organisations the focus will be on the cyber risk management. It is vital to the ABM model to understand the reasoning that underlies the various decision making mechanisms used by organisations to perform their cyber risk management processes. By understanding the reasoning and determining the decision making mechanisms, it becomes possible to understand how organisations decide to invest in their own cyber security.

The research on the behaviour of cyber attackers is limited. This makes it difficult to determine their decision making mechanisms. However, quite some research has been done on the effects that attackers have and classification of attackers. This, along with thinking about attackers as logical entities, makes it possible to reason why attackers attack organisations and how they will choose their target.

Similar to understanding the organisations, it is vital to understand why insurance firms behave like they do. The insurance firms are a key part to this thesis since the main goal is to explore the influence that can be brought forth through insurance policies. Therefore, it is necessary to understand the various decision making mechanisms that insurers utilise as well.

Once the behaviour and interactions of each actor has been determined, the interactions between the actors will be described. Identifying the interactions between the actors is necessary to create a model that behaves similar to the actual cyber security ecosystem. Furthermore, the interaction between insurance firm and organisation is problematic and leads to the many issues that are mentioned in literature (Marotta et al., 2017). Thus it is crucial to identify how these actors interact so these interactions can be modelled properly.

The second sub question is aimed at the insurance policies that are used by insurance firms. The following sub question was formulated:

2. *Which insurance policies can be used by insurance firms and what factors make up these policies?*

The insurance policies used by insurance firms are of great importance to this thesis. This is because the goal is to analyse the effects caused by these insurance policies. Therefore, the possible insurance policies have to be determined so that they can be modelled and used for experimentation in the ABM model.

As was mentioned before, sub questions 1 and 2 are used to understand the ecosystem and to gain information that is necessary to create an ABM model of the cyber security ecosystem. As such, it is important to note that literature will be used to answer these questions and determine what concepts are necessary for the ABM model. The information provided through these sub questions will make it possible to build the ABM model. The ABM model itself will be utilised to answer the last two sub question and to provide the answer to the main question as a result.

The third sub question is focussed on the using the ABM model to experiment and determine what effects insurance policies have on the system. The sub question is formulated as following:

3. *In the modelled system of organisations and attackers, how does the system react to various policy setups employed by insurance firms?*

In order to answer this question, the ABM model will be used. The model will be setup with a configuration similar to the real ecosystem. Experiments are then performed in order to understand the effects of all insurance policies on the system which also includes the effects they have on the total damage. The insights obtained through this sub question will be part of the answer to the main research question.

The last sub question is also aimed at experimentation. The sub question is shown below:

4. *What insurance policies can be designed to lower damages across the ecosystem?*

In the third sub question, the various insurance policies that insurance firms can use to influence the cyber security ecosystem are experimented with. Sub question four follows up on this by identifying possible synergies between various policy options and designing an insurance policy to experiment with. The insight obtained in this sub question will also be used in the answering of the main question.

1.5 Thesis structure

In order to provide an answer to the research question, four sub questions have been formulated. By answering these sub questions the information necessary to build the ABM model and create an experimental design will be obtained. The experiments will provide the information needed to answer the research question. This thesis has been divided into three phases. In the first phase the organisations, attackers and insurance firms will be analysed. In the second phase, the information obtained from the first phase will be used to conceptualise and formalise the agent-based model.

The final phase concerns the experimentation and data extraction from the agent-based. In figure 1-2 a research flow diagram containing the structure of this thesis is shown. The structure of this thesis follows the 10 steps of the ABM modelling cycle (Van Dam, Nikolic, & Lukszo, 2013). The modelling steps are shown by the blocks on the right. In the figure, the input for chapters is shown as well as the sub-questions they answer.

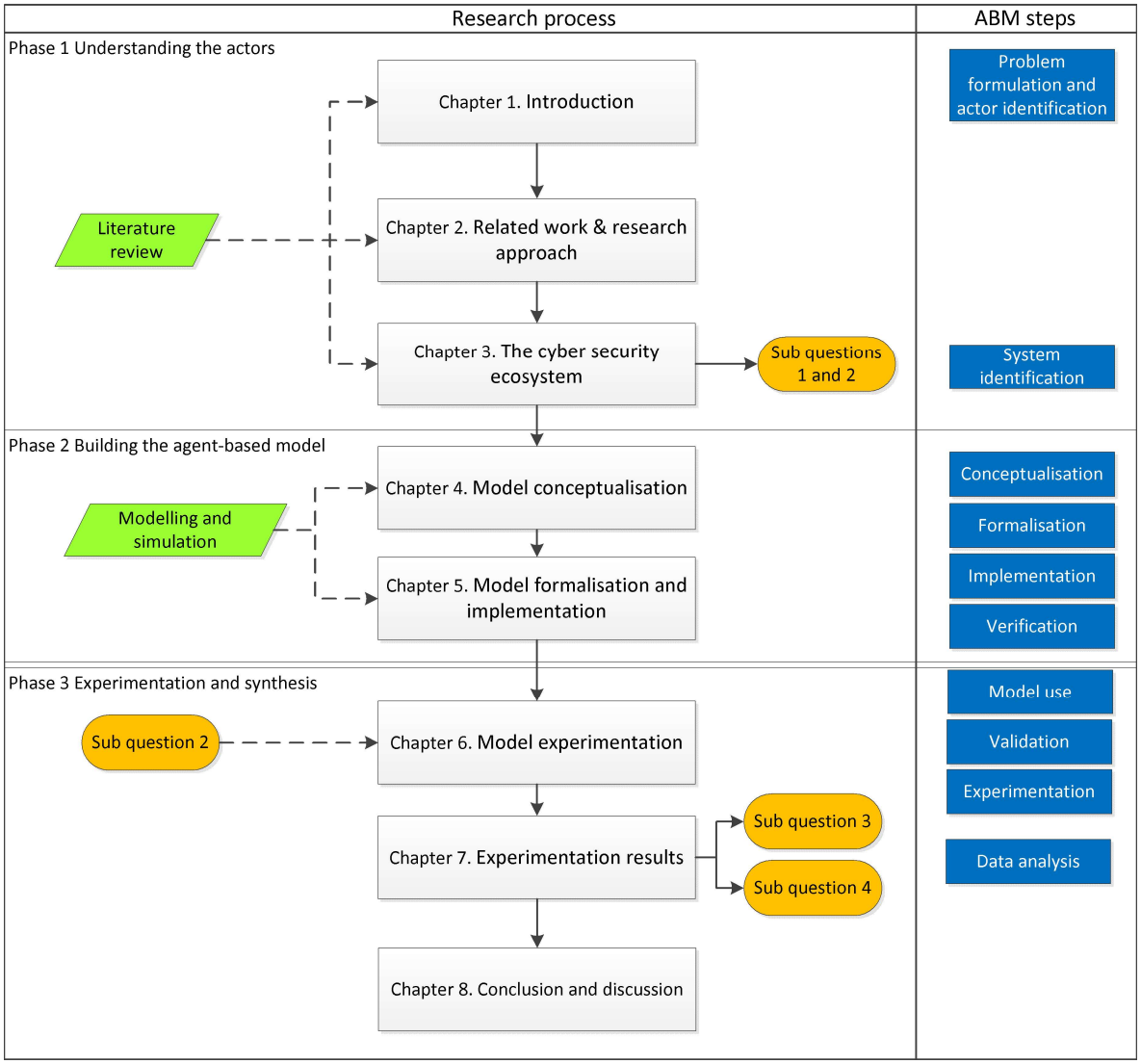

Figure 1-2: Thesis structure research flow diagram

2. Related work & research approach

In this chapter a literature review of research concerning cyber insurance will be described. This literature review is performed in order to determine the state of the art. Furthermore, by discussing the existing literature, a foundation can be created upon which the rest of the thesis can be based. After the literature review, the research approach will be discussed. In the research approach the cyber security ecosystem will be discussed as a complex adaptive system (CAS) and the link will be made to agent-based modelling.

2.1 Related cyber insurance research

In this section prior research on cyber insurance will be discussed. First a short description will be given on the different stances of researchers and their motivations. Second, the research on the effects of cyber insurance will be shown and discussed.

As was mentioned in chapter 1, in scientific literature there are different stances when it comes to whether cyber insurance is beneficial to cyber security or not. Gordon et al. (2003) argues that cyber insurance is necessary and thus useful since perfect cyber-security does not exist, meaning it is the only way to further reduce the cyber-risk an organisation faces. Whilst this is true, investing in insurance also means that an organisation cannot invest that amount in their security. Thus the organisation isn't necessarily more secure as a result of obtaining cyber insurance. However, Bolot & Lelarge (2009) conducted research that shows that insurance can also be a powerful incentive mechanism that can push organisations to invest more in their cyber-security as a result.
Mukhopadhyay et al. (2013) studied the reason why organisations should buy insurance and how insurance can be attractive for organisations. The research shows that insurance can be beneficial for a number of factors. However, it also makes clear that most benefits are financial rather than cyber security related.
One major issue with cyber insurance, and likely one of the reasons it has not seen the predicted growth, is the issue of estimating cyber-security levels in organisations (Jerman-Blažič & others, 2008; Marotta et al., 2017).

In literature several researches have been performed in order to explain some of the effects of cyber security, several relevant papers are shortly discussed below.
A research done by Ögüt, Raghunathan & Menon (2011) studied the issue of estimating cyber-security levels and tried to see how the cyber insurance market can reach an efficient outcome in cyber-risk management through various policies. In their research they found that if insurance firms can verify the self-protection levels of organisations then a specific insurance product and self-protection can become complements to each other. However, when insurance firms cannot verify self-protection levels then insurance and self-protection become substitutes for each other, leading the insurance firm to ask for higher premiums on the insurance. This was also concluded by Yang & Lui (2014), who stated that if insurance firms can observe protection levels then insurance is a positive incentive for security adoption but is a low non-negative incentive when protection levels are not observable. This is very problematic since organisations tend to be secretive when it comes to information like security levels. Additionally, the assessment of security levels is also problematic since it is based in a continually changing environment, security controls that were regarded as very strong in the past start being considered as weak over time as vulnerabilities are found and attackers evolve.
Shetty et al. (2010) studied the effect of cyber-insurance on networks of organisations. In the

research they found that for most parameters the network security worsened relative to a no-insurance equilibrium. This research shows that direct effects of insurance might be beneficial but at the same time leads to a reduction of network security. Pal et al. (2014) studied whether cyber-insurance can actually improve network security. The results show that there are two equilibria, insurance without contract discrimination led to no security improvements whilst insurance with contract discrimination lead to improvement. Contract discrimination means to ask premiums in case organisations don't self-invest in security. However, in the latter equilibrium the insurance firm could no longer make a profit leading to a collapse of the insurance market. In a research done by Johnson, Böhme & Grossklags (2011), cyber-security was modelled through game theory and describes the equilibria involving cyber insurance. The research shows that insurance can be useful and that multiple equilibria exist. This suggests that there is a possible balance in the ecosystem where insurance is affordable and has a positive influence.
Bandyopadhyay, Mookerjee & Rao (2009) looked more closely into the options cyber insurance firms have in order to grow the market. The authors argue that having data symmetry as well as contract discrimination can be positive for the market and lead to cyber insurance becoming a more central part of cyber-risk management.

2.2 Research approach

In this section the research approach will be discussed. As mentioned in chapter 1, the aim of this thesis is to create an agent-based model to simulate the cyber security ecosystem and reduce the knowledge gap in literature. Van Dam, Nikolic, & Lukszo (2013) state that Complex Adaptive System (CAS) thinking is useful to ABM since CAS aspects can be modelled in a natural way into an agent-based model. Therefore, it was decided to use CAS thinking to create the ABM model. Below a description will be given on what CAS thinking entails and how the cyber security ecosystem can be seen as a CAS. After establishing the ecosystem as a CAS, the usefulness and role of ABM will be explained.

2.2.1 The cyber security ecosystem as a complex adaptive system

Complex adaptive systems theory as explained by Holland (1992) can be interpreted as a system that exists out of multiple layers. The interactions in these layers are what makes it possible for a system to exhibit emergent behaviour and can thus be considered a complex adaptive system. The idea behind CAS is that a system is composed of smaller elements that behave, interact and adapt to the environment on their own which causes a system to behave as it does (Lansing, 2003). A system can be considered a CAS when it possesses the attributes: distributed control, connectivity, co-evolution, sensitive dependence on initial conditions, emergent order, far from equilibrium and state of paradox (Chan, 2001). In a CAS there is no centralised control that determines behaviour. The behaviour is derived from the actions and interactions of its components. There is a high connectivity between the components in a CAS. This inter-relation also means that the components influence each other within the system. The components in a CAS are continually adapting to each other and the environment as well. These kinds of systems are also heavily dependent on initial conditions which make them sensitive to input changes. CAS has a high potential for emergent behaviour as well. Far from equilibrium means that a CAS is able to keep thriving and adapting to changes over time, creating new constructs and patterns of relationship. A CAS is also in a state of paradox because it encompasses both order and chaos at the same time.

The cyber security ecosystem can be looked upon as a complex adaptive system since it exhibits these attributes. The components of the cyber security ecosystem are its actors: the organisations, attackers and insurance firms. These actors are individual entities that make their own decisions and interact with each in their own interest. The actors are also inter-related and inter-connected, their actions and decisions affect the other components in the system. For instance, decisions made by the insurance firm can affect organisations and so can decisions made by attackers. Furthermore, the actors in this system are continually adapting to changing circumstances. Attackers are finding new ways to circumvent the cyber controls employed by organisations, whilst organisations continue to adapt to new attacks and defend themselves. The insurance firms are also a product of the evolution of the system because organisations look for new ways to reduce risk. The appearance of cyber security controls can be seen as emergent behaviour of the system. In the system there is also a lot of uncertainty, the behaviour of the system is difficult to predict as are the effects of the actions taken by the actors. Thus looking upon the cyber security ecosystem as a CAS makes sense and can prove invaluable in simulating it.

2.2.2 Agent-based modelling

Simulating a complex adaptive system can prove troublesome since the elements in such a system are complex in nature. Therefore, agent-based modelling was chosen to simulate the cyber security ecosystem. Agent-based modelling is well suited to model complex adaptive systems since these can be modelled in a natural way (Van Dam et al., 2013). This is because ABM uses a bottom-up approach, meaning that the system is modelled from its components, which is similar to CAS theory. ABM makes it possible to model the behaviour, decision making mechanisms and interactions of the components with great complexity. ABM considers the components or actors in the simulation model as agents. The agents are modelled with the behaviour, states and properties that define them in the real system. These elements enable the agents in the model to act, interact and decide on their own similarly to their behaviour in the real system. This allows agents to make decisions based on their own properties and states, simulating their individuality. The states and properties also allow the agents to take on various states as they adapt to changes in the system. As a result, by making the agents interact with each other, the emergent behaviours of the real system will be simulated. This in turn makes it possible to perform experiments on the model to see if the behaviour of the system can be influenced.

ABM can be very useful to simulating the cyber security ecosystem. The ecosystem was already established as a CAS in the previous section which already proves why ABM is well suited. However, there are several other reasons why ABM was chosen in this thesis. In order to model the cyber security ecosystem, three actors need to be modelled: organisations, attackers and insurance firms. Organisations need to be very diverse, since not every organisation would possess the same value of assets or have the same cyber security budget. ABM is well suited to create heterogeneous conditions since agents can be initialised different values for each one (Macal & North, 2005). Organisations also need to be able to conduct a CRM process in which they assess risk and calculate the best options and make decisions accordingly which is possible to model with ABM (Macal & North, 2005). In the cyber security ecosystem there is also a lot of uncertainty, as such the model needs to be capable of introducing chaos for certain variables. ABM is capable of randomising or even modelling probabilities. There is also a need to model a changing environment which can be easily achieved through ABM.

3. The cyber security ecosystem

In chapter 1 a short introduction was given on the cyber security ecosystem. However, in order to fully understand the system and thus to make it possible to create a model that simulates it, it is necessary to gain insight on how each individual actor behaves and how they interact with each other. Therefore, in this chapter the actors in the system of the cyber security ecosystem are described along with their motivations, behaviour and interactions.

In this chapter the answers to the following sub questions will be provided.

1. *What behaviour and decision making mechanisms are part of each actor in the cyber security ecosystem and how do these actors interact with each other?*
2. *Which insurance policies are being used by insurance firms and what factors make up these policies?*

This chapter describes the system composition and interaction and thus is also input for step 2 system identification and decomposition as defined by Van Dam, Nikolic, & Lukszo (2013).

3.1 Actors in the cyber security ecosystem

In order to analyse the effects of cyber insurance policies on the whole ecosystem, it is necessary to understand how the system works and why certain patterns emerge. A system is defined by the actors and their interactions with each other (Van Dam et al., 2013). Thus by examining each actor separately it becomes possible to explain why the system as a whole behaves as it does.

As was explained in chapter 1, there are three actors that make up the system of interest:

1. Organisations
2. Cyber attackers
3. Insurance firms

Understanding the actors in the system can be quite difficult as each actor is subject to several factors and will also act strategically for their own benefit. Van Dam et al. (2012) states that an agent (actor) can be recognised by their boundaries, states, behaviours and ability to interact. The boundaries represent the limits to the actions of an actor. For instance an actor is limited by the budget it possesses or an attacker by its skill level. States show the various internal variables which are used by an actor when taking various actions. These states make it possible to identify the situation of an actor. The behaviours of an agent depict the goals and objectives an actor has in the system. The ability to act determines the different actions that actors can perform. However, besides these characteristics, actors are also influenced through the external environment of the system. For instance, an insurer has to take policies created by the policy maker (governmental entity) into account when designing the insurance packages they will offer. The government regulates insurance in order to create a fair and prospering market and enforces these rules on the market. As another example of an external factor, for organisations cyberattacks could have more effect than just financial losses as it could damage their image as well. This could be very important to an organisation, for instance, iDeal facilitates financial transactions on the web, when they get breached through cyberattacks it could mean that the organisation loses trust which forms the very foundation of the service.
By identifying and understanding the boundaries, states, behaviours and ability to interact for each

actor it becomes possible to understand their decision making processes and thus the behaviour that follows from it.
In the following sections each of these actors will be analysed and described in the context of the cyber security ecosystem.

3.1.1 Organisations

Driving business is the core of every organisation. By doing this they earn money and become profitable allowing it to exist. In order to effectively drive business, organisations perform various activities, from market analysis, customer relations up to product innovation and business expansions. Assets are amassed for and generated through these activities which allow the organisation to compete and increase their market share and thus their profitability (DeAngelo & Roll, 2015; Dowling, 1993). These assets are of great value to an organisation for this very reason. As such organisations face the risk of being attacked not only for their money but also for their assets. The increasing normalisation and integration of ICT technologies in society has also created more risk for organisations as it provided people with ill-intentions to perform cyberattacks (Ögüt et al., 2011). Cyberattacks carry less risk for the attackers as tracing a hacker through the web is difficult and it also doesn't require attackers to be physically present at the location for the attack (Nykodym, Taylor, & Vilela, 2005). As such, cyberattacks are one of the most dangerous risks organisations face (Lewis, 2002).

Therefore, it has become common practice for organisations to perform cyber risk management (CRM) to protect their assets. Cyber risk management is the strategy organisations utilise in order to protect themselves against cyberattacks and thus mitigate cyber risk. Cavusoglu, Mishra & Raghunathan (2004) defines cyber risk management as the purpose to mitigate the risk up to a point where the cost of implementing controls is equal to the value of additional savings from security incidents.

As such, the definition implies that for organisations CRM is all about creating a balance between investments and the savings that result from it. This can be difficult to do as both attackers and defenders are complicated in nature. Furthermore, difficulties can also be found when looking at the possible investments in cyber security. Cyber security is the encompassing term used to describe the various company policies, systems, guidelines, etc. that are utilised to protect assets against cyberattacks (Von Solms & Van Niekerk, 2013). Deciding on what to improve concerning cyber security is a difficult task since there are many different factors to consider as well as many different types of controls that could be invested in (Cavusoglu et al., 2004). Organisations have a limited budget to spend on cyber security as well, thus investing in every cyber security control available is impossible. It is also impossible to attain zero risk because of a changing landscape. Attackers are continually evolving and new vulnerabilities keep being found. As such, organisations have a certain amount of risk that they find acceptable. The organisation determines that investing beyond the acceptable value will actually reduce their gains in the end as it is not worth the investment (Hausken, 2006; Salter, Saydjari, Schneier, & Wallner, 1998). Furthermore, assessing the current state of cyber security is difficult as most vulnerabilities are usually only discovered after a breach has occurred (Rowe & Gallaher, 2006). Investing in controls is also not as straightforward as it seems as the effectiveness of each control is debateable, especially when comparing its performance to controls that are already in use. Moreover, Moitra & Konda (2000) found that there is a curve

observable concerning the survivability of organisations from security breaches, investments in security rapidly increase survivability at first and much slower at higher levels of investment.

Therefore, cyber insurance can be a valuable cyber risk management strategy, since it requires companies to only pay a fixed price to recoup losses as result of an eventual and inevitable cyber security breach (Gordon et al., 2003). Cyber insurance provides organisations with clear insight into the costs and the benefits they get from investing in it. Using cyber insurance in their CRM strategy can lead to reduction of risk towards acceptable levels without the need to invest the entire cyber security budget. Thus the use of cyber insurance could make financial losses actually fall out lower compared to the cost of continuously investing in cyber security. However, one of the pitfalls of cyber insurance is the possibility of the moral hazard occurring, as was also briefly mentioned in chapter 1. The moral hazard refers to the reliance of an organisation on its insurance contract leading to it not investing as much as they can into cyber security controls to stop cyber-attacks in the first place (Hoang, Wang, Niyato, & Hossain, 2017). This ends up with organisations with lower cyber security levels causing them to be successfully attacked more often, however, the organisations do not experience the losses from being attacked as the insurance firm covers it.

The above mentioned characteristics can be used to define the boundaries, states, behaviours and ability to interact. Organisations have only one boundary which is the budget that they have allocated for expenditures on cyber security. This is a boundary as it limits the measures that organisations can buy in order to increase cyber security.
There are several states for organisations: value of assets, cyber security budget, defensive strength of cyber security and own insurance contract. The value of assets is of effect on the risk that an organisation faces since a higher value means that more value can be lost. The cyber security budget affects the measures that can be invested in to increase the defensive strength of cyber security which lowers the risk. Whether an organisation has an insurance contract is of effect on the risk as well, as insurance effectively means that part of the assets is always covered.
The behaviours of organisations consist of accumulating assets and defending these assets against attackers that want to steal it. Organisations also aim at saving money whilst decreasing their risk to acceptable levels.
The actions organisations can take involve accumulating assets, conducting CRM processes and obtain insurance.

The CRM process will be discussed more in-depth below since it is a vital part of the behaviour of organisations in the cyber security ecosystem. Therefore, establishing the CRM process will make it possible to model it in the ABM model.

3.1.1.1 Cyber risk management

As mentioned before, CRM is the process used to assess risk inside an organisation and invest in controls to protect the assets it possesses. However, assessing risk is a difficult thing, especially when there are many factors and uncertainties in play (Ralston, Graham, & Hieb, 2007).

Therefore, several CRM methods have been designed in order to structure the process and give organisations insight into the types of risk they are facing. The strategies differ from each other in the way they structure the process for CRM and the way various risks are classified. As such, the methods all have different perspectives on the risk and vulnerabilities, making each useful albeit in a slightly different way.

The CRM process is very important for the ABM model of the cyber security ecosystem since it is the main procedure for organisations. Therefore, a CRM method will be discussed in this sub-section to make clear what kind of procedure is going to be modelled. For the ABM it is not possible to model every type of CRM method for organisations. Therefore, only several fitting methods will be discussed after which a selection will be made. Based on these methods a CRM concept will be chosen for use in the agent-based model, the conceptualisation of method will be discussed in the next chapter.

There are several methods that propose interesting concepts when it comes to CRM (Cherdantseva et al., 2016). The following three have been selected based on how well known they are and how different they approach CRM compared to each other. These methods will be discussed shortly before a single method is selected to be used in the agent-based model.

- Bowtie
- CORAS
- FAIR

The three mentioned methods all provide a structure for a CRM process that allow organisations to manage their risk. However, each of these methods has a different principle on which the process is structured.

The bowtie method is based on the principles to identify and assess risk, determine acceptable risk levels and design a balanced set of repressive and preventive measures (den Berg et al., 2014). The bowtie method provides a relatively easy structure which can allow organisations to reassess their risk after controls have been applied. However, it also does not go into much detail, leaving the need for additional tools to perform, for instance, cause or consequence analysis (Bialas, 2015).

CORAS is a model-based risk analysis approach and facilitates the integration of several perspectives and focuses on incorporating the context of the system into the analysis as well (Vraalsen et al., 2007). CORAS consists of a method, a language and a computerised tool (UML). The principle behind the method is that the process needs to be understandable for the stakeholders within the organisation. Therefore, the model also relies on graphical visualisation of the risk an organisation faces. The method also provides structure of how to go about assessing the risk in an organisation by describing steps and focus for CRM meetings.

FAIR is based on the principle of identifying and measuring risk. The idea behind FAIR is that without understanding what risk is, what drives risk and standard nomenclature, no risk management method will be truly effective (Jones et al., 2005). FAIR is a method that provides a foundation for this as well as a framework for performing risk analyses. FAIR goes into great detail on how to decompose and measure risk allowing organisations clear insight into the types of risk they face.

From these three methods, FAIR seems most suitable for modelling in ABM. The bowtie provides too little structure to create a CRM process for organisations, whilst CORAS is focused more on facilitating understanding of the risk within organisations to provide effective risk management. Furthermore, FAIR provides a detailed structure for classifying attackers and risk which can also prove useful to analysing the effects of cyber insurance. Below the FAIR method will be explained in more detail to make clear what it entails and how it works.

The FAIR method for CRM

As mentioned before, FAIR focusses on identifying and measuring risk in order to perform CRM. FAIR defines risk as “the probable frequency and probable magnitude of future loss” (Jones et al., 2005). Important is that FAIR sees risk as a probability (chance) and not a possibility (yes or no). As such risk analysis is also all about establishing probabilities.

The FAIR framework consists of four primary components:

- Threats
- Assets
- The organisation itself
- External environment

The combination of these four components makes up the landscape of risk management. Everything within a scenario belongs to one of these categories and can positively or negatively contribute to risk.

Threats are anything that are capable of acting against and asset in a manner that can result in harm (Jones et al., 2005). The method focuses on identifying threat communities and provides structure for this as well in the shape of threat community profiles. In threat community profiles characteristics like motive, sponsorship, capability, personal risk tolerance etc. are considered. A profile helps an organisation to understand the threat agent and can give insight into the probability that they are to attack. There are many characteristics that can be used for building threat profiles. However, more characteristics create only more complexity, whereas FAIR does not have the goal of perfect profiling but instead to gain understanding of the threat landscape. FAIR states that there are four primary components for which threat agent characteristics should be identified (Jones et al., 2005).

1. The frequency with which threat agents come into contact with our organizations or assets
2. The probability that threat agents will act against our organizations or assets
3. The probability of threat agent actions being successful in overcoming protective controls
4. The probable nature (type and severity) of impact to our assets

The characteristics that affect one of these four components are important as they are necessary to understand probability of being attacked, the nature, objective and the outcome of an attack.

Assets are defined within the information risk landscape as any data, device or other component that supports information-related activities and can be affected in a manner that results in loss (Jones et al., 2005). FAIR argues that assets need to have a characteristic that represents value or liability in order to introduce any potential type of loss. There can be many different characteristics that can be at play in organisations. For example an asset could be critical to the organisations productivity, bring along costs for its replacement or cause liability issues because it involves sensitive data.

Assets belong to organisations, where harm to these assets can lead to losses for the organisation and affect its ability to operate. Furthermore, the characteristics of an organisation can attract certain threat communities.

The external environment can play a large role in the threats and risks an organisation faces. The regulatory landscape, competition, etc. can drive the probability of loss.

FAIR risk analysis

FAIR is based on the notion that risk consists of a loss event frequency and probable loss magnitude. By decomposing risk through these components provides a more thorough understanding of how risk is embedded within an organisation.

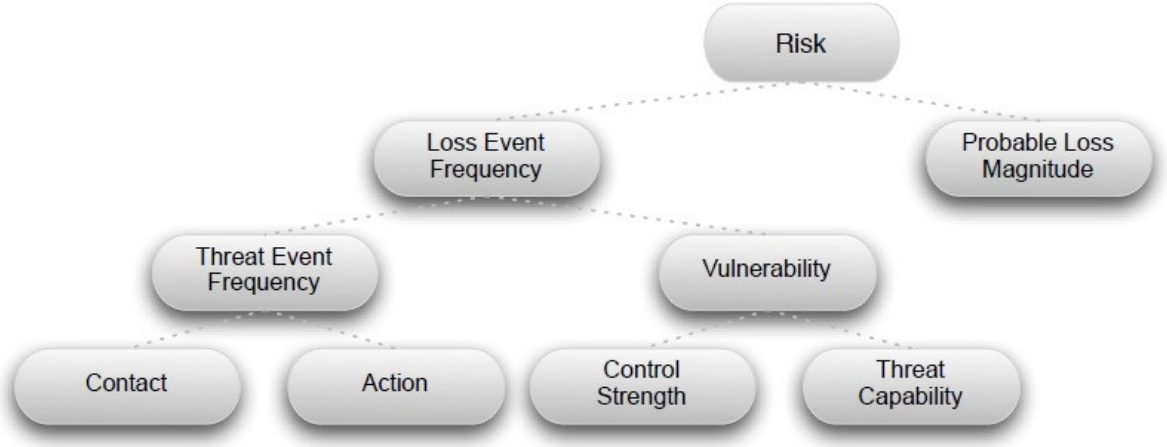

Figure 3-1: FAIR loss event frequency

Figure 3-1 shows the decomposition of the loss event frequency. This tree is related to the attack and defence in the system. The tree shows the frequency of threats occurring whether successful or not, which is further decomposed into the contact a threat agent has with the asset and the probability that an attacker will take action once contact occurs (Jones et al., 2005). The vulnerability that the asset will be unable to resist a threat agent is shown as well. This is decomposed into the control strength to resist an attack and the threat capabilities which indicated how much force an threat agent can apply (Jones et al., 2005).

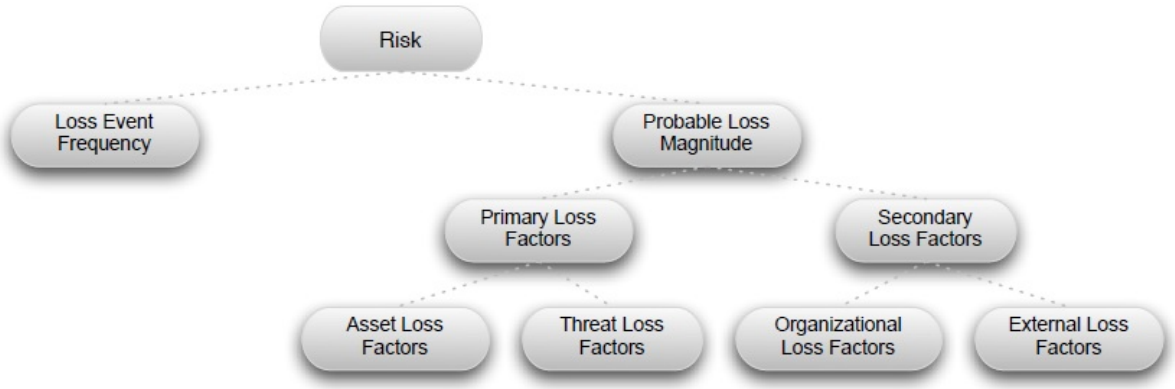

Figure 3-2: FAIR probable loss magnitude

In figure 3-2, the tree for probable loss magnitude is shown. The probable loss magnitude, as one would expect, is focused on the magnitude of loss if an attack has occurred. FAIR states that loss consists of primary and secondary loss. Primary loss consists of asset loss factors and threat loss factors. Asset loss factors focuses on value/liability and volume losses. Threat loss factors focuses on

the way assets are breached, different kinds of breaches can have different consequences concerning loss. For instance, deleting customer information versus disclosing it would have very different magnitude of loss. The secondary loss factors are decomposed into organisational loss factors and external loss factors. Organisational loss factors describe the measures in place when attacks occur, for example, being able to respond quickly can limit losses. The external loss factors focuses on loss that is external to the organisation. For example regulatory/legal instances can fine the organisation, competitors can take advantage of the situation, reaction by the media can cause negative effects leading to losses or external stakeholders can demand compensation or take their business elsewhere.

FAIR determining controls

FAIR states that all controls can be characterised through three dimensions

- Forms
- Purpose
- Categories

The dimensions can help in understanding where controls fit the risk framework, help in assessing control capabilities and in eliminating gaps in the risk management program (Jones et al., 2005).

Controls have one of three forms: policy, process or technology. It is important to keep in mind that few controls stand alone. By understanding interdependencies between controls a greater effect can be achieved.

The purpose of controls refers to them being primarily preventive, detective or responsive. Primarily is mentioned since a control can have several functions allowing it to do more than just its primary focus.

Controls can also belong to a category, which helps in ensuring that gaps don't exist in the controls environment. FAIR mentions three primary control categories: loss event controls, threat event controls and vulnerability controls. For each category controls with different purposes can be selected. Once again, important to note is that a control can have multiple purposes and thus can be cover more than just one category as well.

The control lifecycle is a typical four-stage cycle: design, implementation, use/maintenance and disposal. However, changes in the controls or threat landscape can cause controls to become less effective and thus speeds up the cycle.

Using the elements from FAIR can prove useful to modelling the organisations in the cyber security ecosystem. Modelling FAIR will make it possible to let the organisations assess their risk and thus invest in cyber security in a logical and realistic manner.

3.1.2 Cyber attackers

Whenever someone has something of value, it is very likely that there is someone else that looks upon it with malicious intentions. This is the case in many systems and the cyber security ecosystem is no exception. Organisations possess value in the form of assets which is desired by cyber attackers.

There are many different types of attacks organisations have to face, which makes it difficult to invest in cyber security (Marble et al., 2015). For instance, an attack that breaches the network in order to reroute financial resources is very different from ransomware, for which the company network is held hostage. Furthermore, there is a very broad range of possible motivations for cyber attackers. There are attackers that simply wish to obtain money, but also those that wish to obtain intellectual property, customer data, product data or even simply desire to do damage (Rosenquist, 2009; Verizon, 2018). Where each type of attacker could attack in a different way against which an organisation would have to defend itself.
These differences between attackers as well as attacker capabilities have been addressed in literature as attacker profiles. In attacker profiles the attacker is described along with motivations, time, budget, skills and more depending on the situation (Nostro, Ceccarelli, Bondavalli, & Brancati, 2014; Nykodym et al., 2005). This provides a way to classify what attackers are most probable or are the most dangerous considering the probability of them attacking, providing a way for organisations to focus their investments and reduce their overall cyber risk.

The attacker characteristics mentioned above are very straightforward when it comes to the boundaries, states, behaviours and ability to interact. Attackers do not have any specific boundaries. The states for attackers are made up of the attacker profile of the attacker. The behaviours of attackers are focussed on obtaining assets from organisations and their only action is to select and attack an organisation.

Below attacker profiles and the tools and measures will be further discussed. This will be done because they are major parts of the attacker itself, thus by going more in-depth the information necessary to model these parts can be acquired.

3.1.2.1 Attacker profiles
Attacker profiles are a great help to understanding the types of threats organisations face. By capturing the characteristics of attackers into profiles, it becomes possible to estimate the probability and risk an attacker poses (Jones et al., 2005; Rosenquist, 2009). It is therefore also widely used for cyber risk management (CRM).

There are both internal and external attackers. Internal attackers (insiders) can be large risk to organisations as these employees already have access to the system (Nykodym et al., 2005). Furthermore, they are close to or in contact with the asset on a daily basis and can also be difficult to detect (Nostro et al., 2014). Insiders can be pretty much any employee of an organisation. For example, an operator in the field can be an in insider as this employee is likely to have a certain degree of access making it possible to leak information (Nostro et al., 2014). There are essentially four categories for insider crime: espionage, theft, sabotage and personal abuse (Nykodym et al., 2005). The first three categories are all damaging to the organisation in an obvious way (leaking information or destroying it). However, personal abuse is the use of the company network for personal ends during work hours and thus entails indirect damage in the shape of productivity loss. Besides employees, additional insider threats could be partners and contractors as these too have a certain amount of information or even access that they could exploit (Jones et al., 2005).

There are also quite a few external attackers that organisations have to face. Below a short list is provided (Jones et al., 2005; Rosenquist, 2009).

- Competitor
- Hackers/thieves
- Spies
- Activists
- Nation-state intelligence services
- Malicious software authors
- White hat hacker (ethical hacker)
- Terrorists

Note that the above mentioned list is not exhaustive. Furthermore, for some organisations it can be useful to split some of the mentioned profiles up, for instance hackers/thieves into professional and non-professional. There can be different motivations for attackers to target an organisation. There are attackers that want to steal data/information, do damage, obtain money, test organisations defences, etc.

Attacker profiles make it possible to model more dynamic attackers in the model. This is useful since not every attacker has the same probability to attack. Furthermore, the skill of attackers varies which affects their potential targets as well as their chance to succeed in an attack. For the model that will be built, it is not possible to consider every type of attacker. Therefore, only a selection of relevant attackers will be implemented. This will be presented further explained later on in this thesis.

3.1.2.2 Tools / measures

There are many different ways through which an attacker can attack an organisation (Verizon, 2018). The tools and measures are not restricted to the network completely either. For instance, a thief can steal the password from an employee that has it stored on paper and gain access through that account or an employee happens to see a co-worker forgetting to log-out and use it to commit fraud. Of course, a computer will have to be used eventually in order to actually gain access to the asset. However, in most cases an attacker utilises various software vulnerabilities in order to gain access to the assets in an organisation. There is also a wide range of cyber tools and measures to perform attacks. Attackers can distribute malware, hijack accounts through for instance sending phishing mails, use various software vulnerabilities like zero-day or conduct forceful attacks like DDoS or Brute-Force (Blakely, 2012; Denning, 2000; Libicki, Ablon, & Webb, 2015; Passeri, 2018).

Most of the tools and measures used by cyber attackers have been around for some time. Over the years the software is altered or combined with other techniques to circumvent defences created against it. It wouldn't be too extraordinary that the standard software can be obtained with some ease for cyber attackers, excluding the resources required to operate it. However, there are also tools and measures that are more difficult to obtain. For instance, zero-day vulnerabilities don't come along that often but are obtainable on the black market (Libicki et al., 2015). As such attackers with relatively low resources would not be able to obtain these very easily (Salter et al., 1998).

3.1.3 Insurance firm

In the cyber security ecosystem, insurance firms allow organisations to gain some certainty about their financial losses that occur as a result of cyberattacks. This role is fulfilled by insurance firms in other fields as well. For instance, in the healthcare system, insurance is provided to cover the costs for medical attention when a person falls ill or the car insurance system where car owners are insured in case car related damage occurs by fault of the owner.

Insurance takes a specific shape depending on the market it is introduced in. This is because each market has a specific situation on which insurance is of effect as well as specific conditions to which it must fit. However, at the core, insurance is based on the premise that something might occur unexpectedly and brings a lot of costs along with it. Insurance firms will cover these costs at all time in exchange for fixed continual payments (Bolot & Lelarge, 2009). This provides the person or organisation with some certainty concerning the costs they will occur over time. Note however that this is a simplified explanation, in reality insurance is a lot more complex and in some cases also allows for strategic use as is the case in the cyber security ecosystem.

Insurance firms are the same as other organisations in that they are conducting business and therefore aim to make a profit. The product sold by insurance firms is risk displacement, for which they use policies to indicate what they will cover against a specific premium. Several types of insurance packages are offered, whereas more complete insurance policy packages are sold against higher premiums (Ögüt et al., 2011). Furthermore, in the cyber security ecosystem insurance firms also assess the risk they would have to take on by insuring an organisation which could lead to a much higher premium to be asked if there is much uncertainty or a high chance of the organisation being attacked (Innerhofer-Oberperfler & Breu, 2010). Thus the insurance premium is a tool that the insurer uses to keep every insurance contract it provides viable for their business.

The policies used by insurance firms are made up of several factors. Insurance firms can decide on the premium to be paid, set limits on the maximum amount they will cover and can also differentiate between what types of losses they will cover. Furthermore, insurance firms can also make use of contract conditions in order to protect themselves. For instance, they could demand a minimum investment in controls each year. The premium for insurance is based on the situation. Smaller organisation can obtain insurance for relatively low premiums whilst larger organisations have to pay relatively high premiums whereas the coverage also plays a factor (Herath & Herath, 2011). This has some interplay with the risk the insurance firm would take on as well. It is likely that most small sized organisations will be targeted less often for a lack of asset value, whereas larger organisations operate on a larger scale and tend to possess more valuable assets. The insurance policies will be discussed in-depth in sub-section 3.1.3.1.

Insurance firms also need to take into account the governmental policies prescribed by a governmental policy maker. The governmental policies prescribed by the policy maker are hard requirements that the insurance firms and organisations must adhere to. The policy maker creates guidelines and rules that regulate the market (Böhme et al., 2010). This is done in order to prevent the market from breaking itself and also to protect those affected by its functioning. For instance regulations can be made to prevent insurance firms or organisations from abusing each other leading to an unfair market or to keep the market viable for entry of new insurers. In some cases, the policy maker can also stimulate or make the use of insurance mandatory. These regulations are indirectly affecting the ecosystem and the users of insurance by making it mandatory for them to protect themselves against unexpected costs. This is the case for both the healthcare system as well as the car insurance system in the Netherlands. However, the policy maker is not aiming to control the market but instead the goal is to protect it by enforcing several limits, and conditions (Böhme et al., 2010).

The above mentioned insurance firm characteristics can be used to define the boundaries, states, behaviours and ability to interact. Insurance firms have boundaries enforced onto them by the policy maker. Furthermore, the insurance firms are also limited by their financial balance since a negative balance would mean bankruptcy. Insurance firms have two states: insurance packages available and insured organisations. The behaviours of insurance firms are in essence the same as organisations: to be profitable. As such the insurer will also aim to have a positive financial balance. The actions of insurance firms are to determine a custom premium for organisations based on various variables and to pay-out on insurance claims.

The main method through which insurance firms can influence the ecosystem is through their insurance policies. Because of this the cyber insurance policies will be further explained below. Furthermore, the cyber insurance policies is also the focus of this thesis, thus it is necessary to better understand what possibilities insurance firms have to influence the ecosystem. This information will make it possible to model the insurance firm and its policies in the ABM model.

3.1.3.1 Cyber insurance policies

As mentioned before, insurance firms make use of insurance policies to keep their products viable. The insurance policies contain multiple details that describe when the company is eligible to claim damages from the insurance firm. The policies are in the most basic sense made up of the insurance premium and the coverage. The premium represents the price organisations pay to be insured, as such the insurer can compensate for the risk it takes on by asking a higher premium or they can lower barriers for obtaining insurance by asking a lower premium. The premiums that will be charged to organisations are specifically calculated for each organisation based on their cyber security level, the coverage that is requested by the organisation and the risk the particular organisation faces (Betterly, 2015). Furthermore, as one would expect, the premium is vital to the insurer (Biener, Eling, & Wirfs, 2015). If the insurer asks a premium that is too low they will make a loss on the contract because it is likely that the pay-outs will cost the insurer more than they earn from the premium. On the other hand, a high premium will make insurance undesirable leading to the insurance product not being bought. The insurance firm obtain information about the cyber security level and risk of an organisation by requesting the information or by performing an up-front risk assessment.

The coverage is set-up by the insurer and is priced according to how valuable the particular package is and how much risk it can displace for organisations. The coverage of an insurance package reflects the maximum financial limit the insurance firm will pay-out to an organisation that has incurred a cyberattack. The coverage is split into two parts, first-party and third-party coverage (Betterly, 2015; Hoang et al., 2017; Marotta et al., 2017). First-party insurance is theft and property coverage and covers the damages done to the organisation itself through cyberattacks. Third-party coverage entails the coverage of liability issues that result from cyberattacks. First and third-party coverage is not always offered by insurance firms, some insurance firms only offer liability coverage (third-party) whilst others offer the complete package (Betterly, 2015). The maximum coverage can be a large factor in the decision of organisations to obtain insurance or not. This is because the cyber risk management processes of organisations are built around maximising the gain from their cyber security budget. As such the coverage provided by insurance firms can have large effects on the adoption of it. A high coverage might entice organisations to buy it but can lead to the insurance firm to lose money on the contract. A low coverage will likely make the insurance useless to organisations

as it won't displace much risk (Marotta et al., 2017). Thus it is important that a balance is struck between the premium and coverage in the market.

However, whilst the insurance policy is used to describe the coverage and premium that an organisation will be bound to once insured, there are additional condition that can be employed by the insurance firms for different reasons. For instance, moral hazard can be a large problem for insurance firms (Hoang et al., 2017; Marotta et al., 2017). Moral hazard is the situation where organisations stop investing or greatly reduce investments into cyber security because cyber insurance covers most if not all of the risk. This in turn would lead to a disadvantageous situation for the insurance firm since they would still have to pay-out on insurance claims. Other issues relate to the difficulty to assess and obtain information of cyber security and risk in organisations since there are no real standards for assessment yet, technology changes fast and there are information asymmetry issues (Hoang et al., 2017; Marotta et al., 2017). Furthermore, attacks keep evolving, there is a lot of uncertainty surrounding effectiveness of controls, organisations don't want to share their information and the circumstances of a breach can be hard to verify making it difficult to check whether it is covered by the insurance (Marotta et al., 2017).

In order to handle some of the above mentioned issues or at least to reduce the negative side effects for the insurance firm, certain additions can be made to policies or the process can be altered slightly to gain more accurate information to base the policy on.

Several options will be shown below.

- Risk selection
- Incentivisation
- Integration
- Upfront risk assessment
- Sharing cyber security control information
- Requiring organisations to maintain their security level

Woods & Simpson (2018) mention risk selection as an option that can be used to by insurance firms to protect themselves from the risk they take on from organisations. Risk selection entails discriminating organisations by their cyber security level, increasing the premium the lower the cyber security level of an organisation. Therefore, organisations possessing a low cyber security level will have to pay higher premiums to obtain insurance. This protects the insurance firm by letting them scale the premium they earn by the amount of risk they take on. Organisations that have a low cyber security level will mostly become uninterested as well and reject the offer because of the higher premium. This would prevent the insurance firm from taking on any risks without adequate financial income.

Another option for insurance firms is something called incentivisation (Woods & Simpson, 2018). This option can be used to prevent a moral hazard to come into play in contracted organisations. Incentivisation is the lowering of the premium when the organisation spends on certain specific security controls. In this way the insurer can motivate the contracted organisations to keep improving their cyber security.

An insurance firm can make use of an option called integration, which entails the insurance firm to take on the CRM process for organisations (Woods & Simpson, 2018). This is something that is very controversial since cyber security is a sensitive and thus a confidential subject in most organisations. Therefore, there are likely no insurance firms that offer this nor is it likely to be in demand with organisations. However, this option does provide an interesting prospect, since it could be a good way to keep cyber security levels up and reduce losses to attackers greatly. The reason for this is because an insurance firm has multiple companies contracted and thus has information about effective controls, vulnerabilities and also possesses (more) effective assessment skills.

Insurers can also require something called an upfront risk assessment, this risk assessment is used to accurately determine the cyber security level of the organisation and is performed by the insurer firm (Biener et al., 2015; Hoang et al., 2017). This costs extra for the organisation when opting for insurance for the first time but in return the organisation will receive advice on their vulnerabilities and what controls to buy. Therefore, obtaining cyber insurance will be useful to organisations in the long run but there are higher entry barriers in place.

One advantage of insurance firms is that they have multiple organisations with which they work. As such, they obtain information about the controls used by organisations and what breaches have occurred. This makes it possible for them to aggregate data and become able to advise organisations on what to pay attention to or what measures to take to increase their cyber security effectively. Therefore, by sharing information, insurance firms can provide organisations with the means to more effectively invest their budget into cyber security controls (Biener et al., 2015; Marotta et al., 2017).

Insurance firms can require organisations to maintain their cyber security level as a condition for being insured (Hoang et al., 2017). In this way the insurance firm can make sure that the risk it has taken on does not change too much over time, whilst it also makes sure that the organisation will keep investing in their cyber security.

Whilst the above mentioned list provides several options that insurance firms can employ in their policies, the list is not conclusive. There are likely even more options possible but these haven't been explored or discussed much in literature if at all.

3.2 Actor interactions

There are two situations where interactions between the actors take place. The first occurs in the CRM processes of organisations (investment situation) and the second situation occurs when an organisation is attacked (attack situation).

Investment situation

Organisations keep investing in their cyber security in order to keep reducing risk. This is done through CRM processes in which risk is determined and various options are assessed. During the CRM process the organisations assess the options they have to reduce the risk to acceptable levels. An organisation can determine that cyber insurance might be a viable strategy. For this, it will contact an insurance firm and inquire about the premium it would have to pay and the coverage it will receive. The insurance firm will calculate a custom premium based on the risk the organisation and several other factors depending on their policies. In turn the organisation will use the information obtained to identify whether insurance is the best option to reduce risk. If so, it will formalise a contract with the insurance firm for the specified premium and coverage.

Attack situation

Organisations accumulate value and end up owning large amounts of value, causing them to become targeted by cyber attackers. These cyber attackers will observe organisations to determine in what ways they are vulnerable for attacks. Once an attacker has determined that they are capable of attacking an organisation, it will attempt an attack. The attack will have to breach the preventive and repressive measures that an organisation has in place. This interaction can lead to failure in which case the interaction stops. Or the interaction can lead to success in which case the attacker keeps interacting in order to obtain as much assets as it can before being stopped by the organisation's repressive measures.

The organisation will enter a phase of recovery after being successfully attacked. During this phase the organisation will be on high alert and limit its losses as much as possible. If the organisation is insured, it will also make a claim on their insurance. In turn, the insurance firm will assess the damages and losses and pay out the value that was lost in the attack.

4. Model conceptualisation

In the previous chapter the cyber security ecosystem has been discussed in order to define the system and understand how it works. This has provided an overview of the behaviour of each actor and the interaction that occurs between actors. Making use of the overview it becomes possible to conceptualise the system for the agent-based model. The objective of this chapter is to describe the conceptualisation of the system and the choices made to come to this conceptualisation.

Conceptualising the system involves establishing the agents, link entities, objects and environmental factors that will become part of the agent-based model. The conceptualisation of the system is part of step 2 the system identification and decomposition and step 3 conceptualisation as defined by Van Dam et al. (2012).

The cyber security ecosystem model will be made up of three agents: organisations, attackers and insurance firms. There will be two link entities representing interaction between agents: insurance contracts and cyberattacks. There were no objects that were deemed relevant for the model, thus no objects will be modelled. In the external environment one factor was identified: cyber security effectiveness reduction. In table 4-1 an overview is shown of the model inventory. The elements in the model overview will be discussed throughout this chapter.

Table 4-1: model inventory overview

Model inventory overview	
Agents	
Organisations	Agents that accumulate assets and conduct cyber risk management processes to protect their assets from attackers
Attackers	Agents performing cyberattacks on organisations aiming to obtain assets
Insurance firms	Agents that offer various insurance packages to organisations
Link entities	
Insurance contract	Link that keeps track of the insurance contract an organisations has with the insurer
Cyberattacks	Link that indicates that an attacker has attacked an organisation
External environment	
Cyber security effectiveness reduction	An external factor used to indicate the continual decrease of the effectiveness of cyber security controls

4.1 Agents

As mentioned in chapter 3, there are three agents part of the system of interest: organisations, attackers and insurance firms. The system revolves around the interaction between organisations and attackers. Whereas, the goal of the model is to analyse the effects that insurance firms have on the behaviour of organisations and attackers. Based on the behaviour, relations and interactions described in chapter 3, various states and actions have been identified for each agent. As mentioned in chapter 3, states represent the internal variables of an agent and give insight into the situation of

the agent. The actions show the things an agent can perform to influence their states. The states and actions for each agent will be discussed in the sub-sections below.

4.1.1 Organisations

Organisations stand at the centre of the system. An organisation accumulates assets over time which makes it a target for attackers. Within the cyber security ecosystem organisations concern themselves with defending from cyberattacks. This is done through implementing preventive and repressive controls and policies (den Berg et al., 2014). Organisations have to continually invest in cyber security since cyber security controls become less effective over time. Additionally, attackers also keep improving their skill and develop new tools. Therefore, organisations focus on reducing their cyber risk to acceptable levels (Salter et al., 1998).

For organisations the following states and actions have been formulated.

Table 4-2: States and actions of organisations

Organisations	
States	
Cyber security level	The level of defence against cyber attacks
Budget	The budget that is available to an organisation for cyber security investments
Size	The size of the organisation
Asset value	Value of the various assets that an organisation possesses
Recently attacked	Represents whether an organisation has suffered an attack and is recovering from it
Insurance contract	Indicated whether an organisation has purchased insurance and which package
Actions	
Conduct CRM processes	Process in which organisations determine risk and take appropriate measures to reduce it
Buy insurance	Create a contract with an insurance firm
Recover from cyber attacks	Recover from cyber attacks
Increase / depreciate asset value	Increase / decrease of asset value owned by the organisation

States

Table 4-2 shows that organisations possess six states. Each organisation has a cybersecurity level which represents their perceived security level, ranging from 1 to 5. The security level is based on the security strength, which is modelled as a continual scale between 0 and 1 and shows the exact security level. By using the security strength variable it is possible to simulate the imperfect information that organisations have to work with when determining their cyber security level. This is done by having a scale that translates a security strength value to the respective cyber security level. Budget represents the amount of money that organisations have allocated to cyber security investments. The size of organisations indicate how large the organisation is, this creates differences between organisations as larger organisations tend to have more budget and also more asset value compared to smaller organisations. The asset value represents the value an organisation owns, a part of this value is always at risk of being stolen by cyber attackers. Organisations that have been

attacked will become aware after the attack and enter a state of recovery. The state of recovery is used to simulate the increased awareness after being attacked and the organisation's actions to detect and remove threats from their system. This awareness is represented through the state recently attacked. When an organisation has opted to buy insurance as part of their CRM strategy, they will enter a state of being contracted which is shown by insurance contract.

Actions

Organisations have four actions, as shown in table 4-2. As mentioned before in chapter 3, organisations continually accumulate assets, however, assets also lose value of time (DeAngelo & Roll, 2015). For instance, intellectual property could lose value as competitors manage to create something similar or better. Or for instance, as competitors keep improving, the gap between brands will be reduced which leads to the brand itself being less valuable as well. Therefore, organisations have an action through which they increase and decrease their asset value. After being attacked, organisations will recover from the attack by taking action to prevent further breaches for a certain time period. During this action, organisations attempt to limit their losses as much as possible and are in a higher state of awareness as was mentioned above. Organisations conduct CRM processes in order to assess risk and take measures against it. During the CRM process it becomes possible to determine whether it is beneficial to buy insurance or not. When the organisation determines that insurance is beneficial, they will create a contract with the insurer for an insurance package.

Interactions

There are two interactions that organisations are involved in. First, organisations and attackers interact. The attacker attacks the organisation which can defend successfully in which case nothing happens or it can be breached. When breached the organisation will lose asset value and enter into a state of recovery for an amount of time. If the organisation is insured, it will interact with the insurance firm to make a claim. The second interaction occurs during the CRM processes. In this process an organisation will interact with the insurer in order to obtain a quotation of the premium it would have to pay for each package. If the organisation decides to buy insurance, it will interact with the insurer again in order to create a contract with the custom premium and the insurance package.

Simplifying assumptions

Four simplifying assumptions have been made for the organisations.

The first simplification concerns the asset value of organisations. A single value is used to represent the asset value of organisations. This means that no distinction is made between the different types of asset values thus there will be no behaviour where attackers would target a specific asset value. This was decided since modelling multiple asset values would greatly increase model complexity and impact the time it takes for models to run.

The second simplification concerns the budget of organisations. The budget provided represents only the allocated budget for cyber security processes. Organisations do not have to spend the entire amount. However, left over funds will not be added upon the next allocation of budget. Instead, the budget allocated for cyber security investments is a fixed amount. In this way the allocation of budget is more realistic as organisations always allocate resources based on their money available at certain intervals.

The third simplification concerns the recovery from attacks. When an organisation is attacked it will enter recovery, during which it will only be able recover asset value through means of insurance claims. The organisation enters a recovery state for a specific time during which it cannot be attacked again.

The fourth simplification concerns strategic behaviour of organisations. The organisation will only make use of the CRM process to determine what options to choose. The organisations will not plan ahead and try to take advantage of insurer policies.

4.1.2 Attackers

Attackers, also called threat agents in literature, are the agents that attack organisations in order to obtain assets. Attackers have various characteristics that influence their behaviour. These characteristics have made it possible to create attacker profiles that classify attackers into various groups (Rosenquist, 2009). Attackers utilise many different tools for attacking organisations, where each tool has a different effectiveness and utility in attacks. For instance, ransomware takes an organisational network hostage, whereas a worm is used to gain access to the system (Verizon, 2018).

The following states and actions have been formulated for attackers.

Table 4-3: States and actions of attackers

Attackers	
States	
Attacking	Represents whether an attacker is attacking an target
Attack profile	Profile that determines the skill and resources an attacker possesses
Tool	Tool that the attacker has obtained for its attack
Actions	
Select target	Selecting potential targets
Attack organisation	Attacking an organisation that was selected as target

States

As can be seen in table 4-3, attackers possess two states. Attackers have a state of attacking during which they will attempt to breach the security of an organisation and obtain assets. As mentioned in chapter 3, each attacker also has an attacker profile that states what their skill level and resources are. Depending on their resources they will also be more or less likely to obtain better tools. The tool that is used by an attacker also influences its chances to breach an organisation along with its skill level. Both the tool and skill level determine how much asset value is obtained if the attack was successful (Denning, 2000; Fossi et al., 2011).

Actions

Table 4-3 also shows two actions for attackers. First the attacker selects a target that it wants to attack, based on its skill level. When an organisation has a lower security level compared to the attacker skill, it will select the organisation as a viable target. Afterwards the attacker selects the viable target with the highest asset value for its attack. Before attacking an organisation, the attacker

will determine what tool it can obtain based on its resources. Based on skill and the selected tool it will then attack the organisation. If it is successful it will obtain a part of the asset value based on its tool and skill. If it is unsuccessful the attacker stops its attack.
Decisions were made to allow attackers to have perfect information and thus being able to see what security strength and organisation has as well as the asset value. This choice was made since it is possible for attackers to take their time to identify these aspects before attacking. Furthermore, it is likely that the effect of this choice will have little effect on the results.

Interactions
Attackers have only one interaction: attacking organisations. The attackers interact with the organisation when it decides to attack it. During the interaction the attacker will attempt to breach the cyber security of the organisation. If it is unsuccessful the interaction stops, however, if it is successful the organisation will lose asset value to the attacker.

Simplifying assumptions
Two simplifying assumptions have been made for attackers.

The first simplification concerns the attacker profiles of attackers. For the attacker profiles only two characteristics have been used: skill level and resources.

The second simplification concerns the selection of targets and is related to the attacker profiles. The selection of a target is currently only based on attacker skill level and does not take objective or other characteristics of the attacker into account. Furthermore, the attackers will always attack the viable target with the highest asset value in order to maximise their potential gain.

4.1.3 Insurance firms

Insurance firms are the agents that take on risk of organisations against a premium. For this agent only one insurance firm will be modelled, as the goal is to determine the effects of various cyber insurance policies and not the competition between insurance firms. In the cyber security ecosystem, insurance firms are involved in the CRM processes as insurance is an alternative to investments in controls. Furthermore, insurance provides more certainty as it states what it covers whereas the effectiveness of controls depends on the vulnerabilities it covers.

The following states and actions have been formulated for insurance firms.

Table 4-4: States and actions of insurance firms

Insurance firms	
States	
Premium per package	The premium the insurance firm asks for insurance packages
Coverage per package	The coverage that is provided per insurance package
Risk selection	A strategy where the insurance firm discriminates based on the security level of an organisation
Incentivisation	A strategy where the insurance firms reduces the premium if adequate investments are made by an organisation

Upfront risk assessment	A strategy where the insurance form requires an initial assessment before insuring organisations
Sharing cyber security control information	A strategy where the insurance firm shares the knowledge and experience it has with its customers
Mandatory security level requirement	A strategy which requires organisations to maintain the security level they had when they became contracted
Obtaining premium payments	Receiving payments made by contracted organisations
Actions	
Determine custom premium	Determine the premium a specific organisations will have to pay if it wants to buy insurance
Pay-out insurance claims	Compensate damages that contracted organisations have suffered

States

As can be seen in table 4-4, insurance firms have nine states: premium per package, coverage per package, risk selection, incentivisation, integration, upfront risk assessment, sharing cyber security control information, mandatory security level requirement and obtaining premium payments. The insurer offers three sizes of insurance packages to organisation. Each package contains a base price which is used to calculate a custom premium and an amount of asset value that it will cover. The premium per package represents a value, whereas each package has a different value. The state coverage per package also has a value and is different for each package. Risk selection entails discriminating organisations based on their security level, whereas the insurer can also decide on the severity with which they discriminate against lower security levels. For incentivisation, integration, upfront risk assessment, sharing cyber security control information and mandatory security level requirement, the only states are true or false. This is because each of these strategies can only be applied or not. The incentivisation strategy is used to motivate organisations to keep investing which will lower their premium which can be offered to organisations or not. For upfront risk assessment the insurer requires an assessment to be done before they will provide insurance, thus it can be required or not. Sharing cyber security control information is also the same as the upfront risk assessment, information can be shared or not. The same also goes for mandatory security level requirement since this is also something that can be required by the insurance firm or not. The state obtaining premium payments shows the amount of money is being obtained through insurance payments. As such, it is necessary for the insurance firm to first have contracts with organisations before it can obtain anything. Therefore, for a value higher than 0, this state also signifies whether the insurance firm possesses a contract with an organisation.

See chapter 3 for more information on all the above mentioned states.

Actions

Insurance firms have two actions as can be seen in table 4-4. Insurance firms determine custom premiums for organisations and pay-out insurance claims made by organisations.

Insurers create custom premiums to reduce the risk they accept from organisations. They do this since they suffer from the same lack of information about the cyber security level as organisations, thus the security level is only known in a general sense. Furthermore, if an organisation has a low

security level it also carries more risk. Both of these aspects along with the base insurance price are used to determine the custom premium for specific organisations.

Once an organisation is contracted, the insurer becomes responsible to pay-out on insurance claims made by organisations. The amount that will be paid is limited by the amount that the organisation was insured for, which depends on the insurance package that the organisation bought.

Interactions

The insurance firm interacts only with organisations. The interaction is done during the CRM processes of the organisation as well as after an insured organisation has been attacked. During the CRM process the insurer will calculate the custom premium that the organisation will have to pay if it wants to be insured. If the organisation decides to buy insurance, the insurance firm will also interact during the contract creation process. The pay-out after an attack is a straightforward interaction, the organisation interacts with the insurance firm if it is contracted. The insurance firm will then pay-out the maximum amount or the value loss depending on which is lower.

Simplifying assumptions

One simplifying assumptions have been made for insurance firms.

The first simplification made concerns the insurance packages. It is assumed that the insurance packages are the same for every organisation and that no negotiation is possible. This means that each organisation has the same base price and the same limit to the amount of value insured.

4.2 Link entities

Besides agents there are also link entities. Link entities connect two agents to each other and show that interaction between agents is taking place. For the cyber security ecosystem model, two types of links have been defined: insurance contracts and attacks. Link entities possess states which contain the information exchanged during interactions.

4.2.1 Insurance contracts

The link entity: insurance contract is used in the interaction between organisations and insurance firm. This link entity signifies the contract that is made between organisation and insurer.

The link entity: insurance contract has the following states.

Table 4-5: Insurance contracts states

Insurance contract	
States	
Insurance package	The insurance package that the organisations has purchased along with the custom premium
Contract duration	Amount of time the contract is still valid

The insurance contract link has two states as is shown in table 4-5. The link contains information on the insurance package that the organisation has bought along with the custom premium it has to pay instead of the base premium price. Furthermore, the link also contains the contract duration. The contract duration is reduced every month in the model. Once the duration reaches zero it will cause the link to die thus effectively ending the contract.

4.2.2 Cyberattacks

The link entities: cyberattacks are used to signify that an organisation is being attacked. The link shows that an interaction is taking place between an attacker and organisation.

The cyberattacks links possess the following states.

Table 4-6: Cyberattacks states

Cyberattacks	
States	
Asset value obtained	The amount of asset value that an attacker has obtained in its attack

As is shown by table 4-6, the link entity cyberattacks has only one state. The link entity contains the information about the amount of asset value that was stolen during the attack.

4.3 External environment

The external environment is made up of entities that influence the system but are not part of the interactions that occur within it. Agent entities that can influence the system but are deemed irrelevant for the system of interest are also considered part of the external environment. For the model of the cyber security ecosystem one external environment element has been determined: cyber security effectiveness reduction.

The cyber security effectiveness reduction is an external factor that simulates the aging of controls. As controls age, their effectiveness is reduced since vulnerabilities are found, attackers improve their skills and new tools become available, to name a few examples.

Simplifying assumptions

One simplifying assumption has been made concerning the external environment. The laws and regulations that are enforced on insurance firms will not be modelled. This choice was made since the main focus of the research is to analyse the effects of various insurance policy setups. As such, modelling the laws and regulations would not increase the usefulness of the model by much.

4.4 Model overview

The model as conceptualised in the previous sections can be used to create a model of the cyber security ecosystem. In the model the organisations and attackers act rationally and interact with each other. The way they behave is similar to the real world and therefore, with the addition of an insurance firm, can prove useful to analyse various policy setups. In the model, organisations will rationally decide whether to obtain insurance or not through their CRM processes. This in turn influences their states which in turn influences the actions of attackers. These interactions create emergent behaviour over time thus showing the effect insurance has had.

The main goal of the model is to analyse the effects that various insurance policies can have on the system. In order to identify the effects of cyber insurance, several metrics have been determined and will be measured in the ABM model. The metrics that have been chosen are the following:

1. Average, insured and uninsured security strength
2. Total asset value and value loss
3. Failed and successful attacks

4. Insured and uninsured organisations
5. Insurance firm financial balance
6. Financial balance of organisations

1. Average, insured and uninsured security strength
One factor that is useful to keep track of is the security strength. The security strength represents the level of defence that an organisation possesses against cyberattacks. This metric is divided into three parts: average of all organisations, average of insured organisations and average of uninsured organisations. By keeping track of all three parts it becomes possible to see if insurance has affected security levels and how it changes depending on the packages that are offered.

2. Total asset value and value loss
By keeping track of the total asset value and value loss, it becomes possible to identify how organisations are performing. The closer these two metrics are to each other, the worse the situation is, as the amount of value would become equal to the amount that is lost. Therefore, the effects of insurance will also be observable. Furthermore, the metric can easily be compared for different experiments to see performance of certain setups.

3. Failed and successful attacks
This metric provides insight into the success rate of attacks. Insurance can have various effects, the success rate of attackers can provide a different perspective on the effect of a specific insurance policy setup.

4. Insured and uninsured organisations
The metric for insured and uninsured organisations gives insight into the appeal of various insurance packages. It can show how often an insurance contract is made when a particular insurance policy setup is used. An insurance policy setup that is not appealing enough will not be able to affect the system because it is simply not desirable enough.

5. Insurance firm financial balance
The financial balance of the insurer is used to gain insight into the viability of insurance policy setups. This is a necessary metric since an insurance policy setup where the insurance firm only makes losses will never occur as they seek profits themselves.

6. Financial balance of organisations
The final metric is the financial balance of organisations. This metric keeps track of the expenditure on cyber security controls and insurance and the savings. Keeping track of this gives insight into the effect cyber insurance can have on the budget of organisations.

5. Model formalisation and implementation

In this chapter the model formalisation, implementation and verification will be discussed which are part of steps 4, 5 and 6 of the ABM cycle defined by Van Dam, Nikolic, & Lukszo (2013). The previous chapter described the various states and actions each agent has in the model, the next step is to discuss the narrative and to explain the procedures that are part of the model, which is called the model formalisation. The narrative describes how the model operates and gives an overview of when procedures are executed. The procedures are explained in order to give an overview of what an agent does when executing the procedure and how the procedure affects the states of agents.

5.1 Model narrative

In chapter 3 the behaviour of actors and their interactions where discussed. The actors in the cyber security ecosystem can behave and interact in various ways. However, as chapter 4 already showed, several choices have been made to prevent creating an overly complex model and to still model realistic behaviour despite missing or incomplete information. By describing a narrative it becomes possible to put the choices that were made into perspective and to see how these are incorporated into the model. Furthermore, the narrative can create clarity and explain how the model functions as a whole. The narrative will be described below.

There are five main procedures that create the behaviour and interactions within the model of the cyber security ecosystem. Below a flowchart is presented which provides an overview of the model logics. The flowchart shows how the various procedures are called upon and feed into each other.

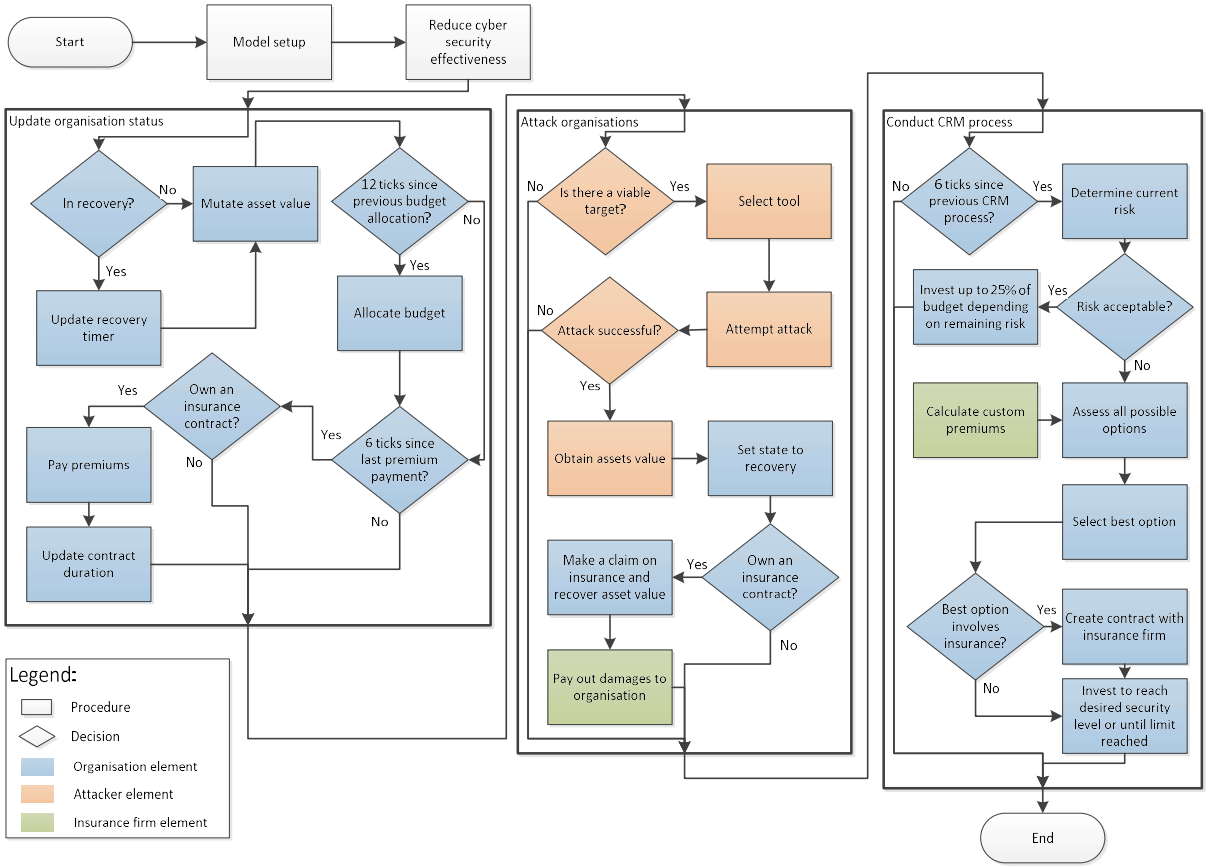

Figure 5-1: procedure flowchart

Figure 5-1 will be discussed below along with the narrative. The procedures will be touched upon lightly in this section and will be discussed more in-depth in section 5.2. The influence of insurance policies on the procedures has also not been shown, these will be discussed in section 5.2 as well.

The first procedure of the model is the setup. This procedure is only performed once in the model before any model runs are done. The setup is used to create all the agents and give them their variables and starting values. During this procedure differences between agents are made to create a more realistic ecosystem. For instance the size of an organisation is assigned and the attacker profile of an attacker is determined.

The procedures after the setup are part of the runs of the model and are performed each tick in the model. A tick represents a month of time, thus each tick is a time step of a month.

The below narrative describes the procedures in the way that they are executed in the model. The procedures are used to influence the various states and to perform actions that have been discussed in chapter 4.

At the start of a run, first the cyber security effectiveness will be reduced. As mentioned in chapter 4, there is a continual reduction of cyber security control effectiveness. The reduction of cyber security effectiveness influences the security strength of each organisation. Three different intensities are possible in this procedure: small decrease, medium decrease and large decrease. This decrease of cyber security effectiveness is also one of the reasons that organisations have to continually invest in their cyber security.

Following the decrease of cyber security are procedures used to update the status of organisations and attackers. In the model first the organisations will check and update their status. This procedure is made up of several sub-procedures. The organisations update their recovery timer, mutate their assets value, allocate cyber security budget, pay premiums and update contract duration. The recovery timer represents the state an organisation has after being breached, during this time they are on high alert and therefore unable to be attacked. The value of assets increase over time as they acquire new assets but at the same time there is a decrease of value possible as mentioned in chapter 4. Every year the organisations will also allocate budget available for cyber security investments. If insured the organisations are required to pay the premiums to the insurance firm as well. Furthermore, they will update their contract duration as well.

Once the organisations have updated their status, one of the core procedures is performed: attack organisations. In this procedure attackers choose their target, obtain tools and attempt an attack on the targeted organisation. Furthermore, when attacks are successful they will steal asset value and cause organisations to go through a procedure in which they enter a state of recovery and make a claim if they are insured.

The following procedure is the CRM process which is again a core procedure, through this procedure organisations improve their cyber security. In this procedure organisations assess the risk they face with the security strength they have and determine whether the risk is acceptable. Depending on whether the risk was acceptable or not they will go through various steps to determine what the best way is to invest their budget. During this procedure the insurer is also involved to determine custom premiums for each package specific for the organisation performing the procedure.

5.2 Procedures

In chapter 3 the cyber security ecosystem was discussed providing information about the behaviour and interactions that make up the system. Chapter 4 followed upon this by discussing the states and actions that will be modelled to simulate the ecosystem. In this section the procedures in the model will be described in detail. The section will explain what the underlying logics and calculations are for each procedure. Furthermore, it will give insight into the way each procedure affects the states of agents in the model.

5.2.1 Setup procedure

As was mentioned before, the setup procedure is only done once, and is done before any of the model runs. This procedure is used to initialise the model and create all agents according to model parameters. The setup procedure can be divided into four parts, the globals and each agent group. For each agent there are several variables that have to be created and assigned to them before the model is ready to run.

Globals

Globals are not part of the agents. Instead globals are variables that every agent is capable of accessing and changing. Most of the globals are used to keep track of values and are utilised by graphs and plots. However, a few of the globals are lists of values that are used by agents based on their state. For instance the skill level and resource level of attackers are contained in lists, whereas the attacker has a profile assigned to it which allows it to determine what skill and resource level they possess.

Organisations

The organisations obtain their states and properties in the setup procedure. In this setup procedure differences between organisations are made through the values assigned to them.

Organisations have one of 3 sizes assigned to them. Size 1 signifies a small organisation, size 2 signifies a medium sized organisation and size 3 signifies a large organisation. The number of organisations of a specific size can be set through parameters on the interface. The size of an organisation is used to determine the value of various other variables for organisations as well. For instance large organisations will have a larger budget and more asset value compared to medium and small organisations.

The annual budget organisations have available for cyber security investments is determined based on the following calculation:

$$A = (r \times B / c + B) \times O \quad (1)$$

With:

- A: the annual budget of an organisation
- r: a random value between 0 and 1
- B: the organisational budget
- c: a constant value set as 2
- O: the size of the organisation

As such organisations of size 3 will have three times as much annual budget compared to organisations with size 1. The random value creates some differences in the annual budget for organisations of the same size providing more realism as no organisation would have the exact same

amount available. However, to keep the differences realistic, organisations can only have up to 50% more annual budget. This is achieved in the formula through a division by the constant value 'c'. The budget is set to the value of the annual budget.

The cyber security level of organisations is randomly chosen from a scale of 1 to 5. It is determined randomly as there is no baseline value that an organisation should start with. Furthermore, organisations rarely possess the same security level. This can be simulated by assigning random values.

Organisations have their asset value set based on the following calculation:

$$V = (r \times M \times D + M) \times O \quad (2)$$

With:

- V: the asset value of an organisation
- r: a random value between 0 and 1
- M: the minimum asset value that organisations can have
- D: the variance of assets between organisations
- O: the size of the organisation

For the calculation, the minimum asset value and assets-variance can both be set on the interface. The minimum asset value serves as the lower bound of the asset value and the variance controls the maximum difference in assets between organisations. The random value is included to create heterogeneity in asset value of organisations of the same size and is capped by the variance of assets. Once again the random value is used to create more realism as no organisation would have the exact same amount of asset value.

The organisations also own a variable called times attacked, this variable is used in the risk calculation of organisations. Part of the risk calculation is based on how often the organisation has been attacked in the past. This variable provides organisations with this history in the setup. The value for times attacked is set through:

$$H = r \times c_1 \times O + c_2 \quad (3)$$

With:

- H: The attack history of an organisation showing the number of successful attacks on the organisation
- r: a random value between 0 and 1
- c_1: a constant value set as 149
- O: the size of the organisation
- c_2: a constant value set to 1

The random value is once again used to create some differences between organisations. A choice was made to let there be at most a history of 150 attacks since this represents a large number of attacks in the model. This was deemed realistic since it would be possible for organisations in the real ecosystem to also have large attack history. The constant value 'c_1' is set at 149 since the constant 'c_2' adds 1 to the calculation as well. The constant 'c_2' was added to prevent the history from ever being 0, thus preventing calculation errors to occur in the model. Furthermore, in the model, organisations are considered as already thriving and active with cyber risk management, thus it is logical that they would have incurred at least 1 attack since their appearance.

A variable called risk acceptance is given to organisations to determine the amount of risk they find acceptable, as was previously explained in chapter 3. The value is a percentage that can be set on the interface. The value on the interface represents the maximum acceptable risk. This means that the value for organisations has a random value multiplied with the acceptable risk to determine how much risk will be acceptable for it.

Attackers
The attackers in the model have several variables. However, only the selection of attacker profile is not straightforward and thus will be discussed. The attacker profile given to attackers determines the skill and resource level they own. The distribution of the different profiles is based on model parameters which can be set in the interface.

Insurance firms
The insurance firms in the model are very simple. The variables they receive are given values through the model parameters which can be changed on the interface.

5.2.2 Reduce cyber security effectiveness

Reducing the cyber security effectiveness procedure is used to simulate the continual degradation of cyber security control effectiveness. As has been discussed in chapter 3 and 4, the reason behind the decrease can come from various factors like new vulnerabilities, new tools, more skilled attackers, etc. (Mukhopadhyay et al., 2013). However, not every factor causes the same degree of reduction in cyber security effectiveness. For instance, a vulnerability being discovered is likely to be much more severe to cyber security than attackers becoming more skilled or new tools. Moreover, vulnerabilities themselves can also have different impacts depending on the kind of vulnerability discovered. Therefore, three intensities of decreases have been modelled: low decrease, medium decrease and high decrease. A decrease of cyber security can be 4% at most for low decreases, 8% for medium decreases and 12% for high decreases. The actual value for the decrease is decided upon through random variables. Furthermore, a chance calculation has been used for a medium or high decrease as these are less likely to occur. By using three different intensities the effects of more severe reductions can be modelled. This makes the reductions of cyber security effectiveness more realistic as major vulnerabilities or new hacking tools aren't very common.

5.2.3 Update organisations

As mentioned in 5.1, there are several sub-procedures part of updating organisations. These sub-procedures are used to update various variables of the organisations. These updates can change the states of organisations or reduce counters that count down to a state change as was mentioned in chapter 4.

The sub-procedure of updating the recovery timer is used to countdown the timer for organisations before coming out of recovery. The timer is determined during the procedure of attack organisations. Once the timer is reduced to 0, an organisation comes out of recovery and is once again vulnerable to attacks.

The allocation of budget for cyber security investments is conducted every 12 months. The budget is allocation is done by setting the budget to the value of the annual budget. Thus, the budget gets overwritten, meaning unspent budget is lost and thus does not count towards the new budget, as

was explained in chapter 4. This also means that there is a limit to the amount of budget an organisation can allocate.

Chapter 4 explained that organisations mutate their assets value since the value of assets decreases over time but at the same time commercial actions of organisations adds upon it. The calculation for the mutation of assets value is done by:

$$V_{new} = V_{old} + r \times c_1 \times V_{old} - r \times c_2 \times V_{old} \quad (4)$$

With:

- V: the asset value of an organisation
- r: a random value between 0 and 1
- c_1: a constant value set at 0.2
- c_2: a constant value set as 0.175

A choice was made to make the effect of reducing the value smaller than increasing the asset value. This choice was made because increasing asset value is one of the main objectives of organisations and it also shows from literature that organisations in general end up increasing their asset value over time (DeAngelo & Roll, 2015). The constant values were chosen based on the patterns it showed in the model. Values were adjusted until a steady increase was observable since this fits the patterns discussed in literature.

Updating contract duration for organisations is a straightforward procedure similar to the recovery timer procedure. The duration of a contract is counted down until it reaches 0, at this point an organisation will enter the state of being uninsured once again.

Organisations that have an insurance contract will also have to pay premiums to the insurance firm. The sub-procedure for this is performed every 6 months. The organisation pays the insurance premium that was calculated by the insurer during the CRM process and reduces its own budget by that amount.

5.2.3 Attack organisations

One of the core procedures in the cyber security ecosystem is the procedure to attack organisations. This procedure is performed mostly by the attackers but for successful attack also involves organisations to perform some actions. The procedure has been visualised through a flowchart to make it easier to understand and follow the steps performed to execute it. The flowchart of this procedure is shown below.

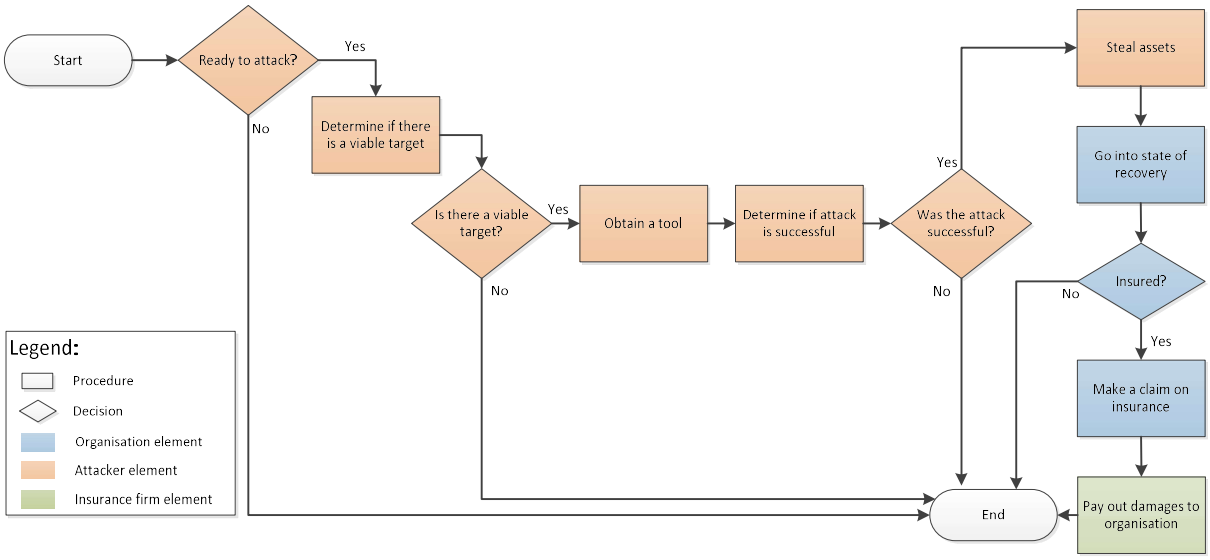

Figure 5-2: Attack organisations flowchart

The procedure is initiated by an attacker. The first step the attacked will take is to check whether it is in the state: ready to attack. If so, the attacker will determine if there are potential targets by comparing its skill level to the cyber security level of organisations. Afterwards it checks whether there are any viable targets, as it is possible that the attacker is unable to find targets available to be attacked (not in recovery) along with a cyber security level lower than its skill. When finding viable targets it will set the organisation with the highest asset value as the target since this target will provide the highest pay-out (Salter et al., 1998). Afterwards it will obtain a tool which will be used to perform the attack. The chance to obtain a specific tool is based on the resources an attacker has and the frequency of the tool (rarity of the tool appearing on the market). Tools have been numbered from 1 to 4 with higher tool numbers resembling rarer tools which are also more effective (Denning, 2000; Fossi et al., 2011). The choice was made to only model 4 tools as to reduce model complexity. Furthermore, too much information about the specific effects of tools is missing making modelling tools difficult. Therefore, each tool is modelled as an increase in effectiveness and rarity resembling actual hacking tools. Tool 1 is always provided for attackers, for the other tools there is chance calculation using the above mentioned frequency and attacker resources. With the tool selected, the attacker is ready to attack and will do so. This leads to a success chance calculation that involves:

- Success chance = breach chance * skill chance * tool chance

This is calculated as following:

$$S = (c_1 - L) \times K \times c_2 \times T \quad (5)$$

With:

- S: the chance that an attack succeeds
- c_1: a constant value set at 1
- L: the security strength of an organisation
- K: the skill level of an attacker
- c_2: a constant value set as 0.2
- T: the increased success chance provided by the tool

The security strength refers to the security strength of the organisation. This value ranges between 0 and 1 is inversed by subtracting it from the 'c_1' to obtain the breach chance. The skill level is a value

for skill that the attacker has in his attacker profile. It was deemed that skill chance should only make add up to 20% to the success chance since it is unrealistic for an attacker to be familiar with all types of systems and defence controls. The tool chance is based on the tool that was selected for the attack.

If the attack is unsuccessful the attacker will end the procedure. If the attack is successful the attacker obtains a part of the asset value of the organisation. This is done through the following calculation:

$$G = V \times (r \times c_1 \times (c_2 + E \times K)) \quad (6)$$

With:

- G: The asset value that is stolen by an attacker
- V: the asset value of the attacked organisation
- r: a random value between 0 and 1
- c_1: a constant value set as 0.4
- c_2: a constant value set as 1
- E: the effectiveness of a tool in obtaining assets
- K: the skill level of an attacker

The tool effectiveness represents the capability for obtaining asset value for the tool. The random variable is used to simulate different amounts of value stolen as not every attack is equally effective. Whereas the constant 'c_1' is used to simulate that only up to 40% of the assets are at stake in an attack. This choice was made because an attacker has a specific goal and tools which make it impossible for it to be able to obtain all asset value within an organisation through one attack. The constant value 'c_2' is used as a base value for the amount of value that can be stolen, whereas, the attacker skill and tool effectiveness can increase the amount that is stolen beyond the base value.

The organisations will reduce their asset value by the amount that was stolen and enter a state of recovery. The recovery is based on a random value between 1 and 6 months since the term needed for recovery is not always the same. The organisation will then check whether it is insured or not. If it is insured it will make a claim on the insurance firm to pay-out the maximum coverage or the suffered damage, whichever is lowest. The amount that was claimed is then added to the asset value of the organisation.

5.2.4 Conduct CRM process

The second core procedure is the CRM process that organisations conduct. The CRM process is used by organisations to assess the risk they face and decide on the investments that can be made to reduce risk. As mentioned in chapter 3, the FAIR framework has served as the base of this procedure. The procedure is mostly performed by organisations but involves insurance firms for calculations of premiums. To make the procedure easier to understand, a flowchart has been made. The flowchart of the conduct CRM process is shown below.

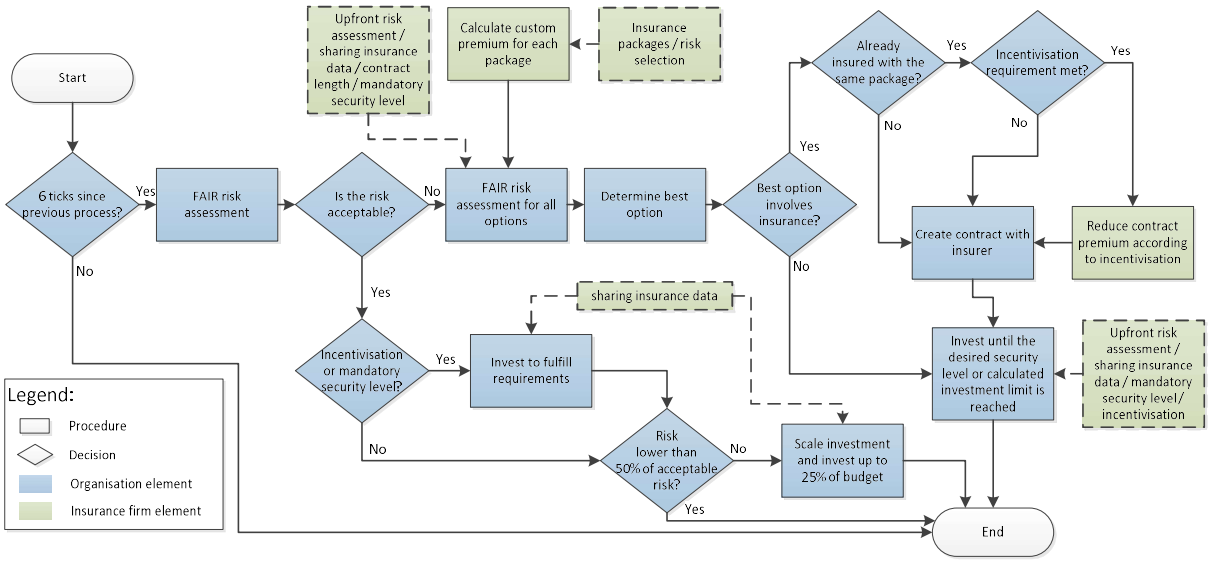

Figure 5-3: CRM procedure

In figure 5-3 the CRM procedure is shown along with the cyber insurance policies mentioned in chapter 4. The squares with striped borders indicate that the insurance policy has an effect on the process.

The procedure is performed every 6 months, which is checked by the organisation at the beginning of the process. An investment period of a half year was chosen since investments by organisations are dependent on several factors. Each investment is conducted as a project made up of assessment, planning and roll-out of improvements. As such it could easily take half a year before another project is started. Moreover, the implementation of ICT related controls can take large amounts of time because it has to be integrated into the existing ICT structure. There is a lot of uncertainty involved when assessing the state of cyber security within an organisation thus research takes longer. The financing of cyber security is another reason why these decisions are not made lightly by organisations and require ample research before a choice is made. As such, an investment interval of 6 months seems realistic.

When 6 months have passed, to begin the procedure, a FAIR risk assessment is done to check the risk the organisation is facing currently. For this assessment, the organisation calculates the various elements of FAIR for each type of attacker. As was mentioned before in chapter 3, FAIR is used to calculate the loss event frequency and probable loss magnitude which can be used to calculate the risk.

Below the calculations for each fair element will be shown.

$$\text{FAIR}_{\text{threat capability}} = \sum_{i=4}^{i} \times K$$
$$\text{FAIR}_{\text{control strength}} = L \times (c_1 + c_2 \times (c_3 - U))$$

$$\text{FAIR}_{\text{action frequency}} = (H + N_i \times F) / H$$
$$\text{FAIR}_{\text{contact frequency}} = (H + N_i \times (r \times c_4 + c_5 \times (c_6 - L)) / H$$

$$\text{FAIR}_{\text{vulnerability}} = \text{FAIR}_{\text{threat capability}} - \text{FAIR}_{\text{control strength}} \quad (7)$$
$$\text{FAIR}_{\text{threat event frequency}} = \text{FAIR}_{\text{action frequency}} \times \text{FAIR}_{\text{contact frequency}}$$

$$\text{FAIR}_{\text{loss event frequency}} = \text{FAIR}_{\text{vulnerability}} \times \text{FAIR}_{\text{threat event frequency}}$$
$$\text{FAIR}_{\text{probable loss magnitude}} = V \times \sum_{i=4}^{i} \times K$$

$$\text{FAIR}_{\text{risk}} = \text{FAIR}_{\text{probable loss magnitude}} \times \text{FAIR}_{\text{loss event frequency}}$$

With:

- K: the skill level of an attacker
- L: the security level of an organisation
- c_1: a constant value set at 0.15
- c_2: a constant value set at 0.05
- c_3: a constant value set at 0.5
- U: the uncertainty in assessing the organisation security strength
- H: history of attacks of an organisation
- N: the number of successful attacks for attacker i on the system
- F: the frequency of an attacker attacking in the system
- r: a random value between 0 and 1
- c_4: a constant value set at 0.12
- c_5: a constant value set at 0.25
- c_6: a constant value set at 5
- V: the asset value of an organisation

The constant values '$c_{1\text{-}3}$' are part of the assessment uncertainty within organisations. The constant 'c_1' represents the minimum security strength that organisations are sure about, whereas 'c_2' is the amount that is uncertain. The uncertainty in assessing security strength can be set on the interface, however, the value 'c_3' is used to make the control strength assessment more realistic by halving the maximum assessment to 75%. This was done since perfect assessment of controls is impossible since there are no standard to compare against and vulnerabilities are usually found by accident. The value of the constant 'c_4' was chosen to be a baseline for the contact frequency. The contact frequency increases according to the cyber security level of an organisation and is limited by 'c_5'. The values for '$c_{4\text{-}5}$' were chosen because they create realistic patterns in the model. The constant value 'c_6' is used to inverse the cyber security level of an organisation for the calculation of the contact frequency. A choice was made to allow organisations to be aware of the number of attacks incurred by organisations of similar size because this usually plays a role in the CRM processes of organisations. The logics being that if a similar organisation has been breached recently than the organisations also has a chance to be attacked and thus has a higher risk (Bolot & Lelarge, 2009).

After the risk is known, the organisation checks whether the risk is acceptable. If it is acceptable, it will assess if it can / has to abide to insurance policies and whether it is useful to invest a small amount (up to 25% of its budget) to decrease the risk even further. Additionally, sharing insured data

can make investments more efficient. This investment is done because it would be very rare for organisations to invest nothing whilst knowing that the effectiveness of security controls reduces over time. If the risk is not acceptable, the organisation will start to assess all possible options it has to reduce risk. The options involve an investment into cyber security controls or combining an investment with one of the three insurance packages. The premium that the organisation would have to pay for obtaining the security packages is calculated by the insurance firm and takes into account their own risk pricing point and the security level of the organisation (Bolot & Lelarge, 2009). For these options any insurance policies in play along with the contract length will also be taken into account. The assessment for each package is done in the same way as the risk assessment and supplemented through a calculation of the predicted cyber security level if the budget was invested alongside an insurance option.

The next step for the organisation is to determine which option comes out as best and thus should be invested in. Note that an organisation is not able to downgrade packages if it is already insured (since this would breach their contract). However, upgrading is still possible.

If insurance was part of the best option, then the organisation will check if it was already using the insurance package option. If it was and incentivisation is in play and can be fulfilled, then the insurance premium will be reduced. The organisation will then create / update its contract with the insurance firm based on the specific package and custom premium that was calculated earlier. Afterwards, it will invest in cyber security based on the desired security level calculated earlier or the investment limits if it couldn't mitigate risk enough or the requirements placed upon it by insurance policies. The investments are also affected by insurance policies that increase efficiency of investments (sharing insurance data and upfront risk assessment)

Then an insurance contract is made with the insurance firm for the specific package and custom premium that was calculated earlier. Furthermore, investments are made in batches until an acceptable risk level is obtained or budget runs out. The investment uses an exponential function with a constant value to simulate reduced return on investment. However, insurance firms can increase the effectiveness of investments by advising organisations or by providing them data. The insurance policy options that can cause this are: sharing insured data and upfront risk assessment. The insurance firms change the constant value that represents the effectiveness of investments.

The calculations are made as following:

$$I = L + ((c_1 - L) \times (c_1 - (e \wedge (c_2 \times P))))$$

Or, with insurance benefits (8)

$$I = L + ((c_1 - L) \times (c_1 - (e \wedge (c_3 \times P))))$$

With:

- I: Investment done into cyber security
- L: The cyber security strength of the organisation
- c_1: A constant value set as 1
- c_2: A constant value set as -0.00004
- c_3: A constant value set as -0.000075
- P: The amount of budget that will be spent

In the calculation the constant 'c_1' is used to inverse the cyber security strength of the organisation. This is done to obtain the remaining cyber security strength that is necessary for perfect security. By multiplying this with the investment function, an increase to the cyber security strength can be calculated. The constant values '$c_{2\text{-}3}$' are the values used in the exponential function as was explained above.

5.3 model implementation

In this section the implementation of the model into modelling software will be discussed. First the selected modelling software will be presented. This is followed by the time step of the model. Afterwards the model interface will be discussed.

5.3.1 Modelling software

There are several options available for modelling software to create agent-based models. For this research the modelling software called 'NetLogo' was chosen. NetLogo was chosen since it is well suited to modelling complex systems developing over time (Tisue & Wilensky, 2004). The software is also easy to understand and often used to create agent-based models. Furthermore, the modelling software lends itself for exploration and experimentation of model behaviour making it a good fit for this research.

5.3.2 Time step

An agent-based model simulates a system over time and because it is simulated over time it is possible to simulate the interactions between actors. NetLogo uses a counter called ticks, these ticks are used to simulate a discrete time step. In the agent-based model built for this research, each tick represents a time step of one month (one tick in the model equals a month). This time step was chosen for two reasons. First of all, the model has to have time steps small enough to let meaningful interaction take place. If a time step is chosen that is too large, for example yearly, then that would mean that interactions only take place every year and that the interaction itself would become an aggregated value of the whole year. This can cause a lot of the details and emergent behaviour to be lost or become very difficult to observe. However, if the time step chosen is too small, it could become very tasking on the hardware to run the model. Therefore, a balance in the time step is necessary. The second reason for this choice is since most of the interactions of organisations can be observed and simulated on a monthly basis. Thus using a monthly time scale will provide all the information necessary for this research. For attackers the time scale matters less as these entities tend to be irregular. However, it is likely that most of the interactions of attackers can also be observed and simulated with a monthly scale.

5.3.3 Model interface

In this section the model interface will be discussed briefly. In figure 5-4 the model interface is shown.

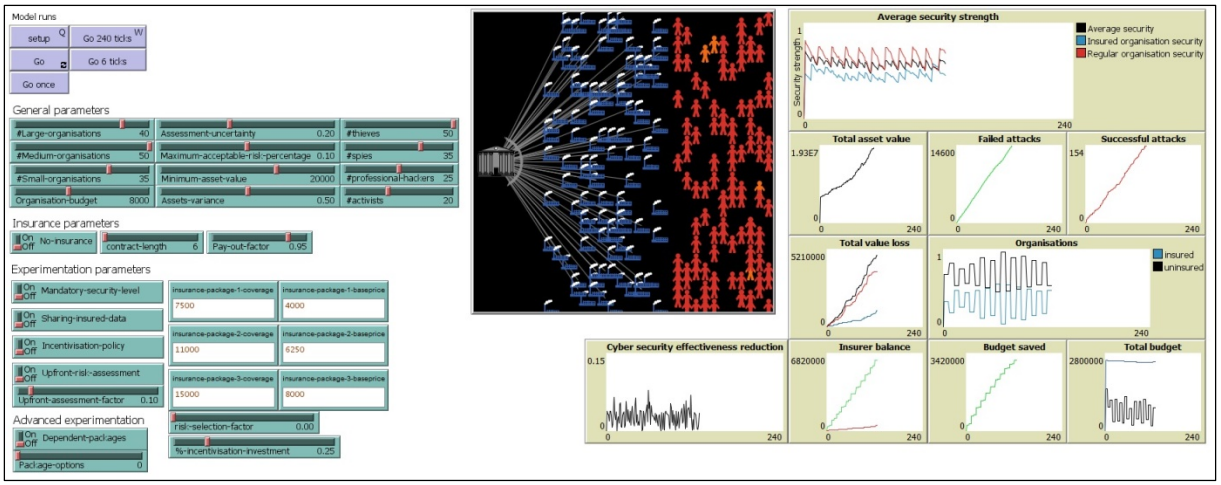

Figure 5-4: ABM model interface

In the model interface there are four distinct items that need to be discussed. The first are the buttons seen at the upper left. These buttons are used to setup the model to prepare it for the first tick and to make the model run a tick represented by 'go'. Additionally the go 240 ticks, automatically setups the model and runs it for 240 ticks. The second item are the green coloured bars and switches seen on the left in the interface. These bars and switches are the parameters that can be adjusted for exploration purposes. The third item are the graphs seen on the right. These graphs contain all the metrics used to measure the performance of the setup. The fourth and last item is the screen in the middle. This box contains the visualisation of the model run and shows the insurer, organisations and attackers, from left to right. Lines between the organisations and insurance firm are made once a contract is established. The lines between the organisations and attackers indicate that the attacker has recently attacked that particular organisation. Attacker turning orange means that they are not ready to attack.

5.4 Model verification

The model conceptualisation showed the intended features and behaviour of the system. Formalising the conceptual model means to translate the behaviour and features into the code that the model will use. During formalisation it is possible that the features and behaviour of the conceptual model are not properly translated and causes the system to behave differently. Therefore, it is important to verify whether the model that was built was also the model that was intended (Van Dam et al., 2013). Verification serves the purpose of determining whether the patterns and emergent behaviour exhibited by the model are part of the system and not caused through translation errors in the formalised model. Thus, it allows for rectification of these errors and make sure that the model built was also the model that was intended.

The verification has been performed for the ABM model used in this thesis, the verification results can be found in appendix A. The model has been corrected according to the results of the verification.

6. Model experimentation

In the previous chapter the model was formalised, describing how the cyber security ecosystem has been simulated through an agent-based model. Furthermore, the model has also been verified showing that the model functions as intended. This makes it possible to explore model behaviour and start experimentation with model parameters. In this chapter the model behaviour will be explored first in order to identify the model sensitivity and to establish a baseline. Following this, the experiment that has been designed in order to answer the research question will be discussed. The chapter will be concluded with a validation of the model. This chapter is concerned with step 7 (model use), 8 (validation) and 9 (experimentation) of the ABM modelling cycle defined by Van Dam, Nikolic, & Lukszo (2013).

6.1 Model exploration

With the model now operational, it becomes possible to explore the behaviour of the system by changing parameters. In this thesis exploration has two functions. The first function is to perform a sensitivity analysis. The second function is to establish a proper baseline that can be used to run experiments with. The sensitivity analysis will give insight into the effect of the parameters on the behaviour of the system. Besides providing information about the effects and sensitivity of parameters, the sensitivity analysis will also provide insight into the values that could be used as a baseline.

6.1.1 Sensitivity analysis

For system simulation models, like ABM models, it is necessary to perform sensitivity analysis. This is because the system can be very sensitive to initial conditions. The initial conditions can magnify each other making seemingly insignificant differences lead to completely different system behaviour (Van Dam et al., 2013). By identifying the parameters to which the model is sensitive, it becomes possible to take it into account when setting up a baseline for experimentation. Furthermore, this will give insight into the parameters that the system is sensitive to which makes it interesting to see if these parameters can be influenced since that could potentially change the behaviour in the system.

Before the sensitivity analysis can be performed, it is necessary to determine the parameters that will be part of the analysis. In chapter 5 the model interface was discussed, the general parameters are of interest to the sensitivity analysis. However, since computational power is limited, it is not possible to include every parameter of interest in the sensitivity analysis. Therefore, a selection has been made of input variables that could prove to be sensitive. The parameters that will be tested are the following:

Table 6-1: sensitivity analysis setup

Parameters	Value range	Step size
Organisation-budget	5000 - 20000	2500
Assessment-uncertainty	0 – 0.5	0.1
Maximum-acceptable-risk-percentage	0 – 0.2	0.05
Minimum-asset-value	5000 - 30000	5000

It is very difficult to determine values for the parameters of the cyber security ecosystem since there is very little information available that hasn't been aggregated. Therefore, the values chosen are based on estimates and rely on the balancing of variables on each other in the model in order to achieve realistic patterns. The patterns were deemed realistic when they showed expected

behaviour and showed similarities to the aggregated data on the cyber security ecosystem, this will be discussed further in the validation (section 6.3). The budget of organisations, assessment-uncertainty and maximum-acceptable-risk-percentage are interesting for the sensitivity analysis. This is because these parameters influence the decision making processes of organisations and thus influence the system through their behaviour. It is likely that if there are parameters that show high sensitivity then it would be one of these four parameters.

The remaining parameters that can influence the system are the insurance packages, contract length and pay-out-factor of insurers. The table below shows the values selected for these parameters.

Table 6-2: sensitivity analysis static parameters

Parameters	Value
#Large-organisations	40
#Medium-organisations	50
#Small-organisations	35
#thiefs	50
#spies	35
#professional-hackers	25
#activists	20
Asset-variance	0.5
Contract-length	6
Pay-out-factor	0.95
Insurance-package-1-coverage	7500
Insurance-package-1-baseprice	4000
Insurance-package-2-coverage	12000
Insurance-package-2-baseprice	6250
Insurance-package-3-coverage	14000
Insurance-package-3-baseprice	8000

For the sensitivity analysis the number of organisations and the number of attackers are not that interesting to vary with. This is because the impact of these changes would be very obvious. More organisations mean that a specific organisation would have less chance to be attacked unless there were too few organisations for attackers to attack in the first place. Having more attackers would lead to organisations getting no rest and losing more value.

For the rest of the parameters it was decided to exclude these from the sensitivity analysis because they are part of the insurance firm. This means that parameters will be used for experimentation or that the effects of these parameters are of less importance to the sensitivity analysis. The values shown in table 6-2 were chosen since they allow for realistic behaviour to occur. The contract-length has been set at 6 months since this will prevent organisations to be bound to their insurance contract thus allowing for a better analysis of the sensitivity of variables. The pay-out factor has been discussed previously in chapter 4. In this chapter it was explained that the pay-out factor parameter was added because the insurer pays out less than the actual damages because of the difficulty of assessing the damage. The value of 0.95 was chosen to represent the inaccuracy of pay-outs. The insurance package coverage and base prices have been chosen to represent decent insurance package amount depending on an average asset value (15000) and organisation budget (10000). The average was determined as the mean values of the parameters.

A separate additional sensitivity analysis will be performed to determine tipping points for the insurance packages. By determining tipping points, insight can be obtained into the balance within insurance packages and see how it affects adoption of insurance. For this test the minimum acceptable risk will be set to 0, this will make organisations make choices based on the insurance package alone and not their acceptable risk which will highlight the sensitivity only to the insurance packages. Furthermore, only one insurance package will be used for analysis. The following values will be used for the analysis.

Table 6-3: tipping points analysis setup

Parameters	Value range	Step size
Insurance package 1 - premium	5 - 14005	2000
Insurance package 1 - coverage	250 - 21250	3000

The model will be run for 240 ticks which represents 20 years in the model. This time period was chosen because cyber risk management is a slow process. The investments made in cyber security take time to be implemented since it usually involves modifying the IT infrastructure within the organisation. Furthermore, part is this thesis is to analyse the effects of cyber insurance over time. With a time period of 20 years this would be possible.

6.1.2 Sensitivity analysis results

In the previous section the setup for the sensitivity analysis was discussed. Based on the parameter values selected, a sensitivity analysis has been performed. In this section the data obtained from the sensitivity analysis run of the model will be discussed.

The sensitivity analysis was performed as a full factorial experiment. This means that every combination of the selected values for each parameter has been run in the model. For instance, every value for the organisation budget has been used in a run with every value of the assessment uncertainty. This type of experimentation provides the most insight into the influence of each parameter. For each combination it is also necessary to perform multiple runs in order to obtain a reliable dataset for analysis. This provides a large amount of data combined with the full factorial approach. Therefore, the data has been analysed through to use of R program (R Core, 2018) using the package ggplot2 (Wickham & Chang, 2008). R was selected because it is a powerful tool that is both simple, efficient and includes a large number of tools that can be used for analysis. This makes it very well suited to analysing large amount of data.

Below a summary of results obtained from analysing the data will be provided. The full sensitivity analysis can be found in appendix B. For this summary only the most relevant figures will be presented. The sensitivity analysis was performed using the metrics for cyber security strength, annual budget and global value loss because they would provide the most information concerning sensitivity of parameters. The insurance package tipping points analysis was tested on the number of insured organisations and is shown below as well.

Cyber security strength

There are three cyber security strength metrics that were used for analysing the sensitivity: global, insured and uninsured cyber security strength. The choice was made to include all three since the sensitivity can display itself differently based on the situation (insured or uninsured).

The sensitivity analysis on the global security strength showed that the pattern is the same no matter the parameter settings. Furthermore, only the budget of organisations showed any sensitivity. In figure 6-1 the graph on the effect of the budget of organisations on the global cyber security strength is shown. In this figure it can be seen that for lower budgets lead to lower cyber security strength in the model, whilst high budgets lead to high cyber security strength. This is a realistic behaviour, since a lower budget means that there is less money to invest in controls and it might even prevent organisations from being able to afford cyber insurance. Furthermore, it seems that for higher budgets, the spread patterns are overlapping quite a bit. This means that having more budgets does not increase the cyber security strength in equal steps. This is likely caused by organisations reaching an acceptable risk and thus refraining from investing large amounts. Other than the budget of organisations there was very little difference between parameter values. For the cyber security strength of insured and uninsured organisations, the same behaviour was observed. Only the budget had an observable effect on the cyber security strength. As such, it can be said that there is some sensitivity for the budget but this was to be expected and can be explained logically.

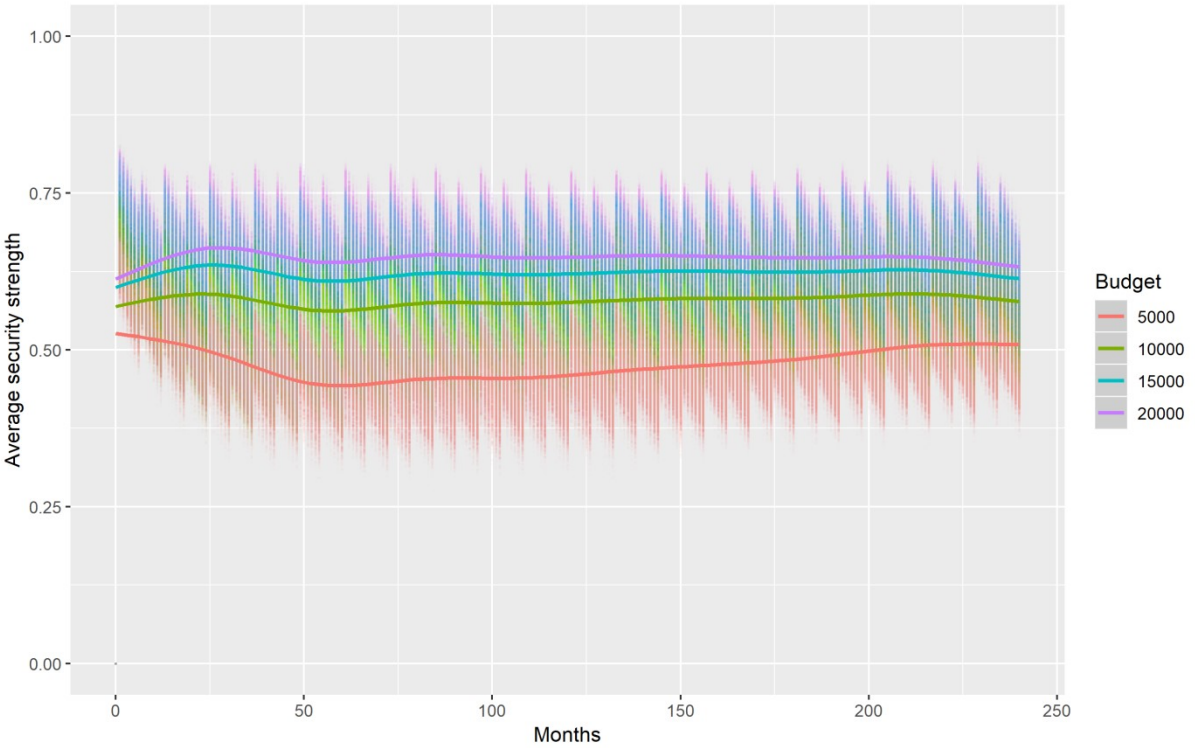

Figure 6-1: The effect of organisation budget on the global cyber security strength

Total annual budget

Organisations allocate budget for cyber security investments each year, their annual budget. This metric is interesting to analyse for sensitivity since the annual budget influences expenditure on cyber security controls and thus influences all other output variables.

The first thing noticeable in the analysis of the annual budget was that there was quite some spread between runs. However, this was mostly cause by the organisation budget (figure 6-2) and maximum acceptable risk percentage (figure 6-3). As can be seen in figure 6-2 the budget has a lot of sensitivity which was to be expected since the metric is the annual budget. Thus for a high budget, the values start high and vice versa for a low budget. In figure 6-3 it can be seen that the starting points follow the budget parameter values. Furthermore, for each maximum acceptable risk percentage

differences can be observed. For low maximum acceptable risk, the annual budget increases or stays quite constant whilst shifting the parameter value higher leads to lower annual budget or smaller increases. This is logical since the maximum acceptable risk percentage determines how much risk is acceptable. Thus finding no risk acceptable would lead to increasing the budget until risk is completely mitigated, whilst find a lot of risk acceptable has the opposite effect. The other parameters showed very little differences between runs which means that there was little sensitivity.

The behaviour that was observed is all logical and expected. There is sensitivity to the organisation budget but this was to be expected since it is directly related to the annual budget. The maximum acceptable risk also proves to have an effect but its effect is very logical because it relates to the risk that organisations want to reduce.

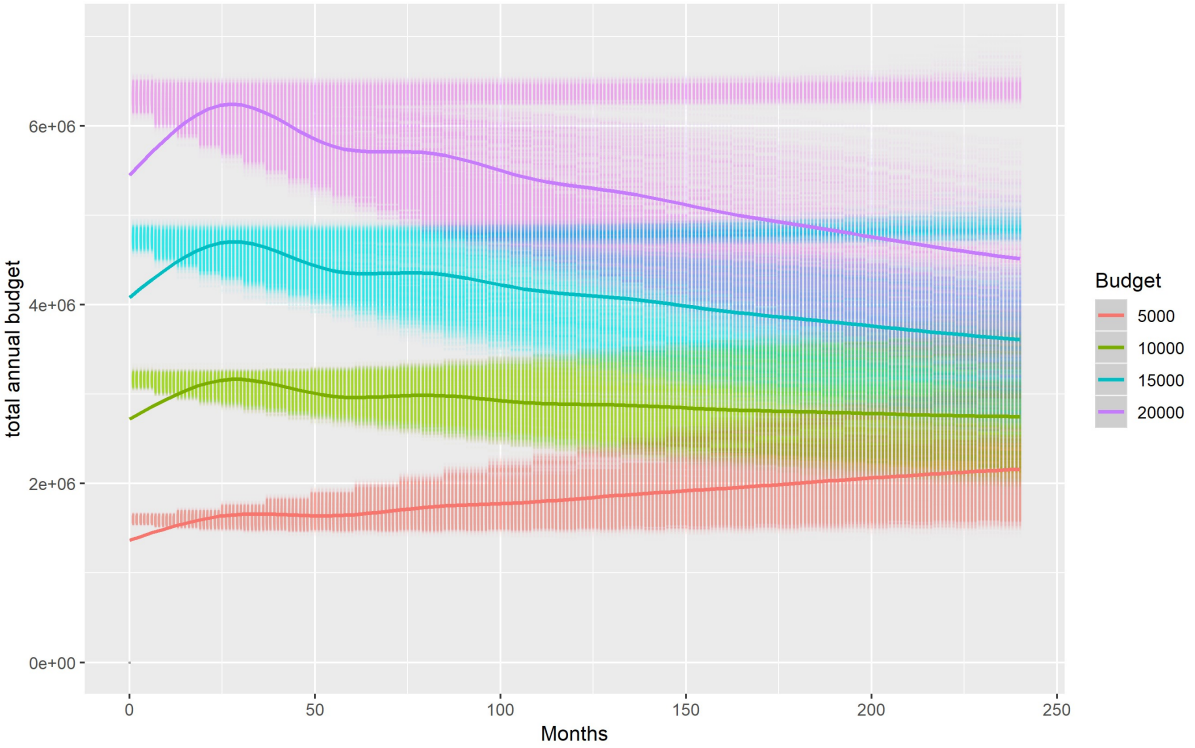

Figure 6-2: The effect of organisation budget on the total annual budget

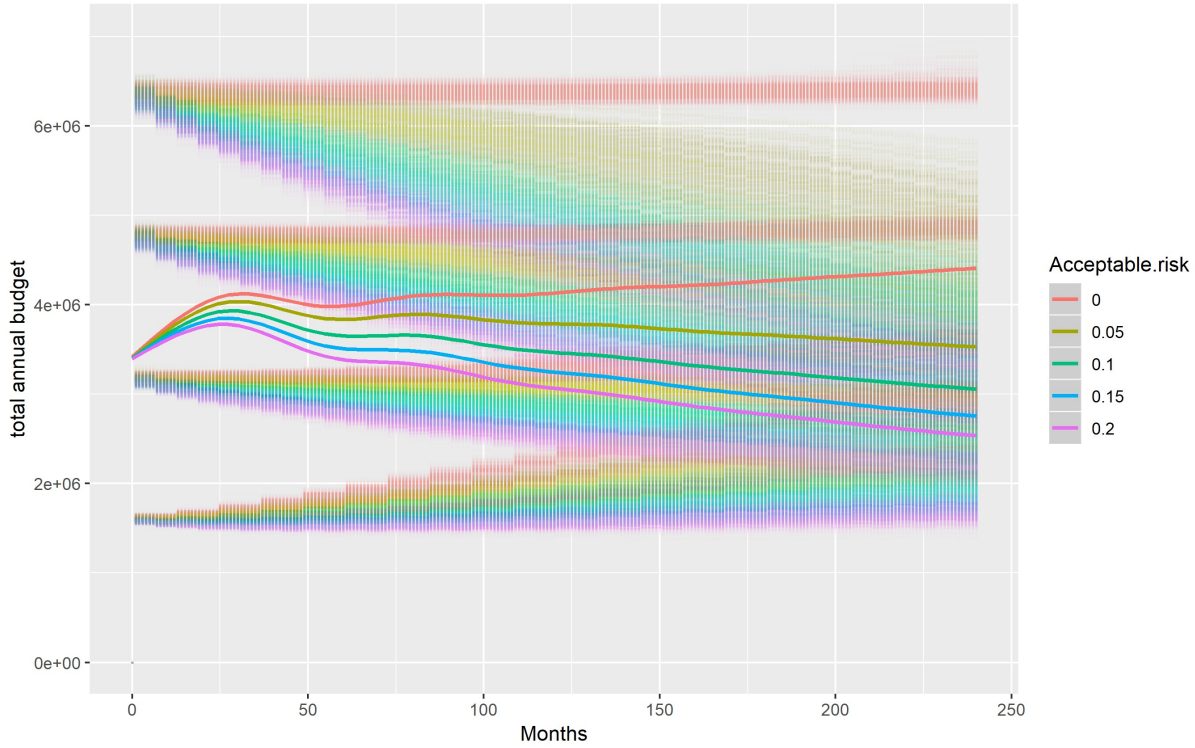

Figure 6-3: The effect of maximum acceptable risk percentage on the total annual budget

Global value loss

The global value loss shows how much value is stolen over time. This metric is interesting for analysing the sensitivity since it keeps track of the most important value in the cyber security ecosystem, asset loss to attackers.

In figure 6-4 the most interesting graph of the global value loss analysis is shown. This figure shows the effect of the minimum asset value on the global losses of organisations. As can be seen in the graph, the model is quite sensitive to the minimum asset value when it comes to the asset losses. This is to be expected since the minimum asset value determines how much assets an organisation has and thus how much an organisation can lose. The spread in the graph is attributed to random variables used to make organisations more heterogeneous at initialisation of the model. Therefore, this too is expected and logical. The other parameters had some effect but these were too small to consider them as sensitive.

The only parameter that the global value loss is sensitive to is the minimum asset value. However, this sensitivity is logical and expected and will not be problematic for the model.

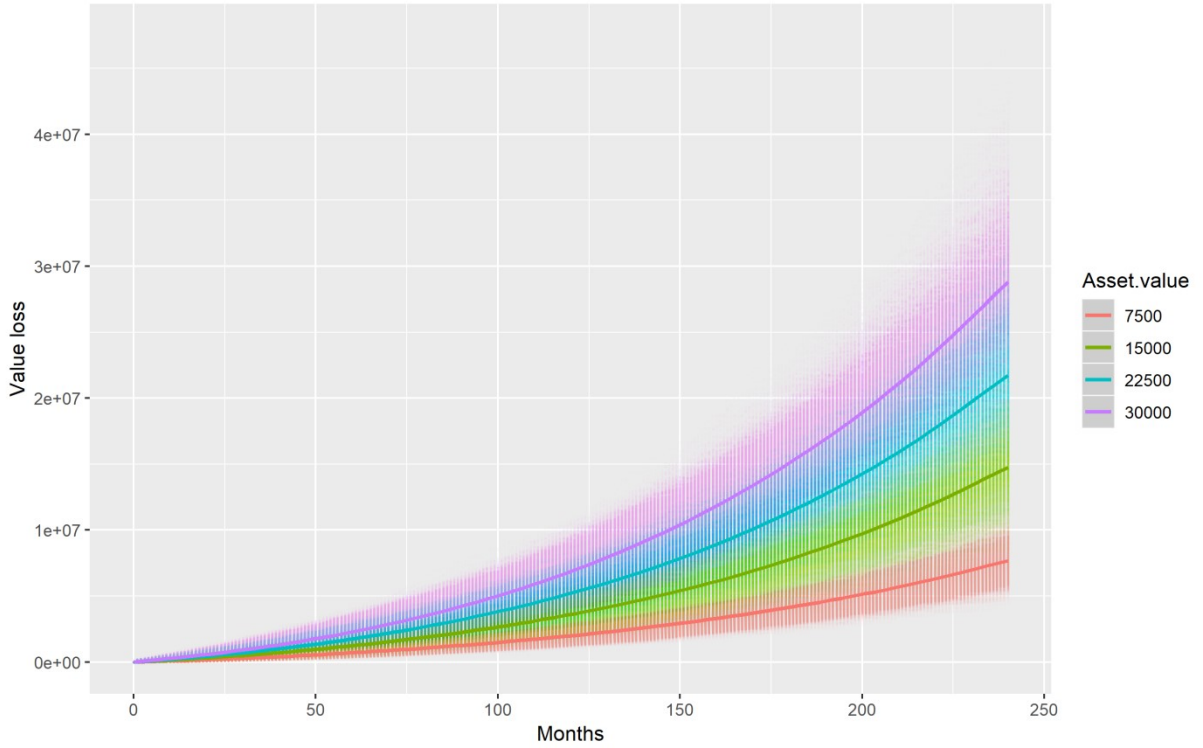

Figure 6-4: The effect of minimum asset value on the global value loss

Insurance package tipping points

Tipping points can indicate a balance between parameters and show the limits to certain effects. The metrics of interest to tipping points of insurance packages are the number of insured organisations. The number of insured organisations can indicate how appealing an insurance package configuration is.

When looking at figure 6-5 it can be observed that for a lower premium the adoption of insurance is much higher leading to all organisations to be insured. This is logical behaviour since for a low price it is always useful to organisations since the organisation doesn't have to pay a lot to obtain it. This makes it a very viable way to reduce risk and save as much budget as possible. For the coverage the effects are less pronounced but the effects are still similar. Lower coverage leads to fewer organisations being insured since it does not provide enough coverage for what it costs. This makes high coverage more appealing. The downward curves can be explained by the behaviour of organisations. In the model, organisations will prefer not having a contract if there would be no difference between investing in cyber security itself or having insurance. Thus over time as asset value increases and organisations have continually improved their cyber security, insurance will be less effective and can be dropped by some organisations. As the premium increases this effect becomes more pronounced since there is more to gain by dropping insurance. The coverage makes the premium less of a barrier to organisations, but once again, if organisations deem that investing money directly is more advantageous, then they will drop insurance. This also explains why the runs converge in the coverage graph. The organisations eventually have more asset value which makes investing the budget worth more than buying insurance. Furthermore, because there are three types of organisations with asset values corresponding with their size, the ending point is consistent over runs because medium and large organisations likely outgrow the coverage which leaves only small organisations to be insured. Tipping points for the premium can be found at around 10000. At this

point increasing the price further will give little effect. The tipping point for the coverage can be seen at 15250. At this point, providing more coverage doesn't have any large effects on the adoption of insurance.

The behaviour seen in the figure is not unexpected. The behaviour can be explained through the decision making of organisations and partially by modelling decisions that were made.

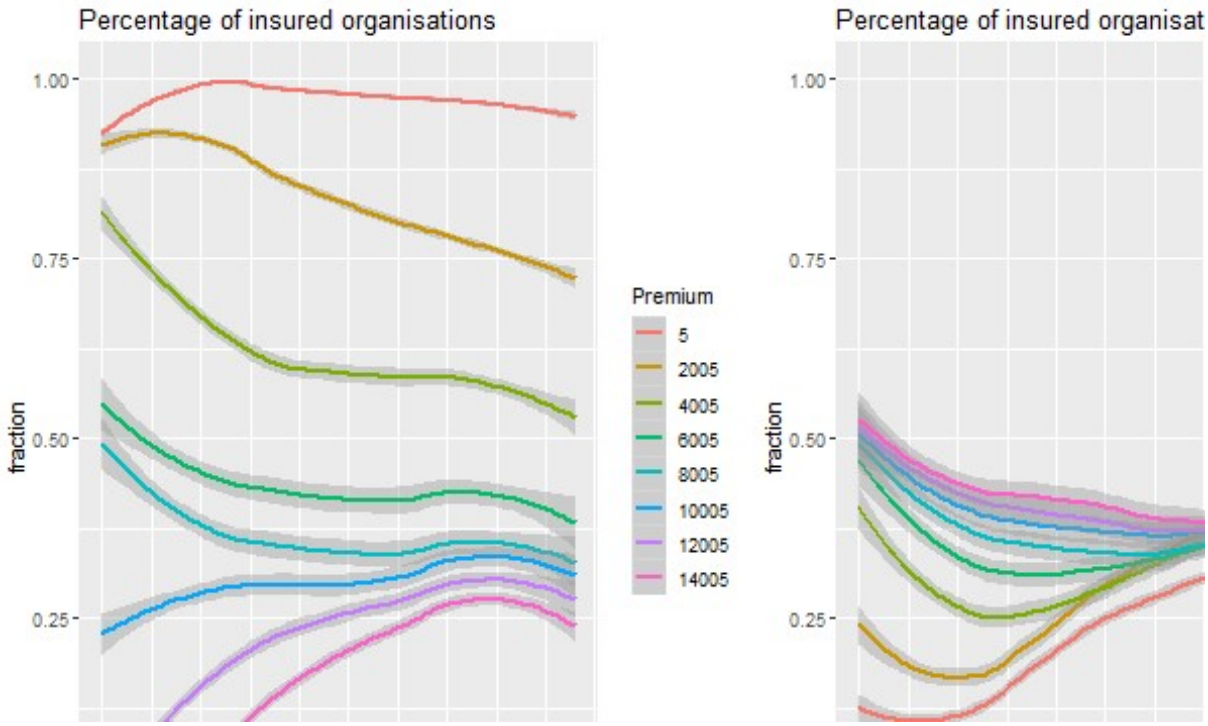

Figure 6-5: Tipping point analysis of premium asked and coverage offered

6.1.3 Model baseline

For the general parameters a baseline has to be established in order to perform experiments. This is necessary as it makes it possible to replicate the experiments and is also necessary to be able to compare the results of the experiments to each other. Based on the performance of the system and the sensitivity analysis results discussed above, a baseline has been determined. The parameter values for the baseline will be discussed below.

Insurance package options

Whilst, the insurance packages will also be part of the experimentation, it is also a parameter that is always active in the model. Therefore, a baseline value for the insurance package needs to be selected. For the packages a value of 4000, 6250 and 8000 have been selected for the premium price. For the coverage the values 7500, 11000 and 15000 have been selected. These values were selected since they create realistic behaviour, with values not becoming too low or high. Furthermore, these values correspond to the budget that organisations have, making the most expensive package difficult to obtain for smaller organisations but being a relatively big investment for large organisations which is very logical. The coverage has been set proportional to the price and also corresponds to the asset value of organisations.

Contract length

Similar to the insurance package options, contract length is also always used in the model. Therefore, for the contract length a baseline value also has to be established. The value that will be used for contract length is 12 months. This value was chosen since yearly contracts is a regular thing in the business world. Therefore, it would not be odd that insurance firms use the same standard.

Number of organisations

A choice was made to make the baseline for the number of organisations: 40 large organisations, 50 medium organisations and 35 small organisations. This distribution was logically chosen because most organisations are medium sized. These organisations have not reached beyond the border much and tend to possess smaller budgets compared to large organisations. It, therefore, makes sense to have the highest number of this organisation size. However, there would also be reasonably many large organisations. The larger organisations can be considered multinationals that expand beyond borders and companies with relatively higher financial resources. Since they are multinationals, this makes them targets everywhere in the world that they have a presence or branches. Thus they become part of the cyber security systems in multiple countries. There would be fewer small organisations, since these organisations usually grow into medium organisations quite fast or disappear. Furthermore, small organisations are targeted less often because of a low presence and asset value making it a logical choice to have fewer small organisations.

Organisation budget

The budget of organisations will be set at 8000. This budget was chosen since it creates a realistic pattern in the model as was also observable in the sensitivity analysis results. One would expect that organisations would be able to keep the budget relatively constant throughout years. However, it would also not be strange to see increases or decreases as long as they are not too extreme (for example, after 20 years the budget has risen to 150%). A value of 8000 for the organisation budget can achieve this behaviour.

Assessment uncertainty

The value for assessment uncertainty will be set at 0.2. This value is chosen since it creates a reasonable amount of uncertainty when it comes to assessing the security strength in the organisation. Furthermore, assessing the security strength has always been a difficult thing to do, since there are no standards, effectiveness of controls cannot be measured, possibilities of vulnerabilities to be found and since the attackers continually develop. Therefore, an uncertainty value of 0.2 seems logical.

Maximum acceptable risk percentage

For the maximum acceptable risk percentage the value will be set at 0.1. This signifies that 10% of assets at risk can be acceptable for organisations. However, the actual value is between 0 and 10% and is decided upon through a random variable. Therefore, it seems logical that at most 10% of assets at risk could be acceptable, since the maximum value would rarely occur anyway. It is much more likely that lower values will be chosen.

Minimum assets value

Based on the sensitivity analysis the minimum assets value that will be used as the baseline will be 20000. This value was chosen because it allows for organisations to begin with a decent amount of asset values which in turn influences the amount of risk they find acceptable. This creates a realistic situation with more dynamic behaviour of organisations compared to lower values.

Assets variance

Assets variance refers to the difference between organisations of the same size in their asset value. The value for the variance will be set at 0.5, which means that organisations can have up to 50% more asset value above the base. There is no particular reason for this value other than creating variance between organisations since it is not logical for organisations to have the exact same asset value. By using 50% the difference between organisations seems reasonable. Note that the value means up to 50%, through the use of a random variable the exact percentage is determined.

Number of attackers

For the attackers the numbers will be set at: 50 thieves, 35 spies, 25 professional hackers and 20 activists. This distribution was chosen since the most active attackers would be the thieves (Passeri, 2018; Verizon, 2018). After that there would be quite a number of spies, which for this research also includes the attackers that want to steal IP. Thus a number of 35 spies seem reasonable. The professional hackers appear at a much lower rate compared to thieves and spies, as such 25 seems like a logical amount. Activists are rather uncommon and thus it seems logical to have a lower value than professional hackers (Passeri, 2018; Verizon, 2018). Therefore, a number of 20 seemed logical. Furthermore, the number of attackers has been balanced on the model, where this setup provides realistic patterns.

Pay out factor

The pay-out factor is used to indicate the damage assessment difficulties the insurer has to face when determining the damage for the pay-out as was mentioned in chapter 3. For this factor the value 0.95 will be used. This means that 95% of the damage is paid whenever an organisation is breached. The value of 95% seems logical, since most of the damage would be easily assessed whereas it is the details where assessment becomes difficult.

6.2 experimental design

The focus of this research is to see what the effects are of various insurance policy solutions on the cyber security ecosystem as a whole. Particularly there is an interest on the effects of cyber insurance on insured and uninsured organisations and on the positive effects various insurance policies can provide. In order to gain this insight an experimental design has been created which describes and explains what experiments will be done.

Several options that can be used by insurance firms as part of their insurance policy have been discussed in chapter 3. These options have been implemented into the agent-based model and can be used for experimentation with the model. This research is aimed at performing an exploratory study of these options and to see if certain combinations of these options can bring forth positive effects for the organisations and the insurer.

However, it is not possible to setup an experiment with all values of all the experimentation parameters as this would simply make the experiment too tasking and would result in the experiments to take too much time to run with the available resources. Furthermore, it would end up providing an extreme amount of data making analysis difficult and tasking to perform. Instead a selection of experimentation parameters has been made along with a restricted set of variations. This selection was chosen because it is likely that these experimentation parameters have the largest effect and thus will provide the most interesting results.

The experimental design has two sets of parameters that will be used for experimentation: static parameters and experimentation parameters. In the previous section the baseline was discussed, the baseline values are the input for the static parameters. These values have been determined through the sensitivity analysis and through logical reasoning to provide a realistic system setup to experiment with. This makes the results from experimentation meaningful since it would mean that the observed patterns and effects in the model are more likely to occur in the actual system as well. Experimentation on the system is done through experimentation parameters that will be varied. By varying the parameters, the system can be tested against different values of the parameter thus giving insights into the effects of it. The experimentation parameters that have been selected will be discussed below.

Insurance package options

The insurance package options are made up of two components: premium price and coverage. These components will be discussed below.

Premium price

The price of the premium is one of the most obvious parameters that insurance firms can use to influence the cyber security ecosystem. As was mentioned in chapter 3, the premium represents the price organisations pay to be insured and can have a large effect on the viability of the insurance firm and on the adoption of insurance in the system. Therefore, not every premium value is useful for experimentation since it would simply not be viable for the insurer. Thus there are upper and lower limits which provide a value range that can be used for experimentation.

There are nine premium price values that will be used, and three packages that will be experimented with. The values that will be used are the following.

Table 6-4: Premium price values for experimentation

Parameters	Setup 1	Setup 2	Setup 3
Insurance-package-1-baseprice	2000	4000	8000
Insurance-package-2-baseprice	3125	6250	12500
Insurance-package-3-baseprice	4000	8000	16000

For the first package setup the values are 2000, 3215 and 4000. The second package will have the values 4000, 6250 and 8000. The final package has the premium price values of 8000, 12500 and 16000. These values were chosen since they represent an upper and lower bound as well as a baseline value (setup 2). This will provide insight into the behaviour of the ecosystem when the premium price is varied. Furthermore, it will allow for insight into the synergies of the premium price with other insurance policy options. The setups will correspond to the setup options of the insurance coverage which is discussed below.

Coverage amount per package

The coverage of an insurance package reflects the maximum financial limit the insurance firm will pay-out to an organisation that has incurred a cyberattack as was explained in chapter 3. The limit of the pay-out can be a large factor in the decision of organisations to obtain insurance or not. Similar to the insurance premium option described above, for this variable there is also an upper and lower limit. This is because coverage that is too high might result in losses whilst coverage that is too low will be unattractive to organisations.

For the coverage nine values have been selected, three for each package that will be used for experimentation. The following values have been selected for experimentation.

Table 6-5: Premium price values for experimentation

Parameters	Setup 1	Setup 2	Setup 3
Insurance-package-1-coverage	2500	7500	12500
Insurance-package-2-coverage	6000	11000	16000
Insurance-package-3-coverage	10000	15000	20000

The values selected for the first package setup are: 2500, 6000 and 10000. The second package will have the values 7500, 11000 and 15000. The third package will provide organisations with values of 12500, 16000 and 20000. These values were chosen because they provide an upper, lower and baseline value for the coverage. Through these values, insight can be obtained about the saturation of the market for the specific insurance packages. Furthermore, the combination of this variable with other options might yield unexpected effects. As mentioned above for the insurance premium packages, the setups for the coverage correspond to the setups for the premiums. This means that setup 1 is a combination of the setup 1 of coverage and premium.

Contract length

The contract length for insurance contracts can have varying effects on the behaviour of the organisations. This is because it forces organisations to be contracted for the duration and thus pay for their contract. Therefore, organisations have to take into account the premiums they will have to pay over the year when deciding on their investments to reduce cyber security.

For the contract length the values 6, 12 and 24 months will be used. These values were selected since they can give insight into three situations. The value 6 allows organisations to determine whether they will obtain insurance during every CRM process that they conduct. This provides them with the ability to drop and obtain insurance whenever they want. However, the values 12 and 24 show the situation where the organisation has to plan ahead and reserve budget for insurance premium payments. The values 12 and 24 were selected because it allows for experimentation with short and long term contracts. Furthermore, having contracts of excessive length (e.g. longer than 24 months) are unlikely to occur in the ecosystem since these require long term commitment from organisations. Whilst this parameter might have limited effect by itself, in combination with other insurance options it might show unexpected results. Furthermore, since it is an easy parameter to set by insurance firms, it makes it useful to experiment and see whether it can become beneficial to the insurer and organisations.

Risk selection
As was explained in chapter 3, insurance firms can make use of risk selection to protect themselves from the risk they take on from organisations. This is done by discriminating against the cyber security level and asking higher premiums is the security is low.

The values for this option consists of a range of values that determine the severity with which insurers discriminate against lower cyber security levels, as was mentioned in chapter 4. Three values have been selected for experimentation with risk selection: 0, 0.25 and 0.5. These values were chosen because it provides a baseline through the value 0, for which risk selection is not used, and can provide information on the effect when higher numbers are used. It was purposely chosen not to include extreme values since this is likely to only make insurance too expensive in the first place, thus it would become similar to having a higher premium price. This variable will mostly provide insight into the viability of cyber insurance in the market since it will show whether an insurance firm can exist even if it doesn't discriminate based on cyber security level. Furthermore, it can show if discriminating against organisations can improve organisations in general. This is because insurance would mostly be viable if organisations already possess a decent cyber security level leaving the other organisations to keep investing in their own security causing them improve it.

Incentivisation
Incentivation involves lowering of the premium that an organisation has to pay when the organisation spends their budget on certain specific security controls as was explained in chapter 3. However, for this research, incentivisation will not require specific controls to be bought but instead will simply require investing in cyber security by the contracted organisation.

For this option there is once again only a yes or no possible as was mentioned in chapter 4. Incentivisation can be of use to give cyber insurance a more positive effect on the cyber security levels of insured organisations which makes it interesting to experiment with. Furthermore, there could be synergies with other options which could potentially amplify the positive effects it has.

Upfront risk assessment
In chapter 3 the upfront risk assessment option was discussed. Making use of an upfront risk assessment can provide insurers with additional information on the security of an organisation and allows them to give advice on vulnerabilities.

For this option there is only a yes or no state possible as was explained in chapter 4, the value for the upfront risk will be 0.1 multiplied by the insurance price. The costs were chosen as a constant value since it would not change for different packages. However, the organisation size would matter in this case since the larger the organisation the more connected it usually is. Thus there would be more costs involved. This option is relatively easy for insurers to implement. Furthermore, it gives the insurance firms a way to actively contribute on top of the coverage. Therefore, it is interesting to experiment with it and to see if it can (together with other options) provide a positive influence on the ecosystem for organisations and insurance firms.

Sharing cyber security control information
Insurance firms gain valuable information from the organisations that they have under contract as was explained in chapter 3. The information can be shared by the insurance firm to help organisations make better or more effective decisions (Biener et al., 2015; Marotta et al., 2017).

As was mentioned in chapter 4, the values for sharing cyber security control information would be a yes or no, where the yes state would have an effect on the effectiveness of investments. This option is interesting to experiment with since it involves something only an insurance firm has, experience and knowledge of the cyber security of multiple organisations. Therefore, it would be logical for an insurance firm to try and leverage this in order to provide organisations with additional benefits, which in turn is also beneficial to the insurance firm since it would reduce the number of successful cyberattacks. Thus learning more about the effects of sharing information and whether it provide substantial benefits on its own or as a synergy with other options could prove valuable.

Requiring organisations to maintain their security level

The last option that will be used for experimentation is the requiring of contracted organisations to (at bare minimum) maintain their security level as it was when they entered into a contract (Hoang et al., 2017). This option was discussed previously in chapter 3.

As was mentioned in chapter 4, for this option there is only a yes or no possible. This option is interesting since it can provide organisations with a floor in cyber security level, meaning that they will not go lower than what they already have. Therefore, as organisations face more risk and upgrade their security, when the time comes to make a new contract, then they will be required to maintain a higher security level than at the start of the model runs. It is also likely that this option can create a synergy with some of the other options, possibly creating a larger effect.

6.3 Model validation

It is very important to validate the model since this will determine if the model is fit for its purpose (Van Dam et al., 2013). Fit for its purpose means that the model is capable of providing valuable insight into the system of interest. There are several methods that can be used to validate models. However, many of these are not applicable to the ABM model built in this thesis. This is because there is very little data available on the cyber security ecosystem which can actually be used for model validation. Most of not all of the data available has been aggregated, thus the specific values necessary for the ABM model cannot be derived from it. Therefore, in order to still be able to validate the model, the individual concepts of the model can be validated instead (Augusiak, den Brink, & Grimm, 2014). By validating the individual concepts of a model, the structure of the model can be called valid which indicated that the system that makes use of these concepts is automatically also valid. This is very well suited to ABM models as well since these involve CAS thinking meaning that the model was built by modelling the components and concepts that make up the system in order to simulate the emergent behaviour. Therefore, by validating the concepts of the model, the model itself will be validated as a result. In order to validate the concepts, the patterns created by runs of the concept parameters can be identified. The identified patterns will then be compared to the behaviour that was expected from it in literature. The goal is to determine whether there are any differences between the patterns and what was expected. If there are differences, then it is also important to understand why these differences occurred. Additionally, the concepts that cannot be measured will be discussed with regard to literature for their validation. Before the concepts can be validated it is necessary to establish the concepts and the expected behaviour.

The concepts that have been used in the ABM model and need to be validated are the following.

- Appreciate / depreciate asset value
- Reduce cyber security effectiveness

- Cyber security investment curve
- Tool frequency, success chance and effectiveness

Each concept will be discussed below along with its validation.

6.3.1 Appreciate / depreciate asset value

The concept of appreciating / depreciating of asset value is used by organisations to mutate their asset value. This asset value can be increased by organisations in various ways. For instance, the corporate image of a company is counted toward the asset value and is actively managed by most organisations (Dowling, 1993). However, maintenance is required otherwise it will devaluate over time. DeAngelo & Roll (2015) also mention that peaks and troughs are possible when it comes to asset value. However, over time an increase in the asset value is expected.

In figure 6-6 the graph showing the global asset value in the system is shown. This run was done with the same setup that will be used for the experimentation. The data consists of 432 experiments and lead to a total 2160 runs of the model being done. The graph shows a gradual exponential growth. This is to be expected since there are various ways in which organisations can obtain asset value. Furthermore, there is a slight shift up and down observable from time to time. These are the same peaks and troughs as mentioned by DeAngelo & Roll (2015). The patterns are likely to become even more pronounced if fewer organisations are used. The graph shows very similar behaviour to what was expected, thus way this model concept was implemented is valid and will contribute to a more realistic simulation of the ecosystem.

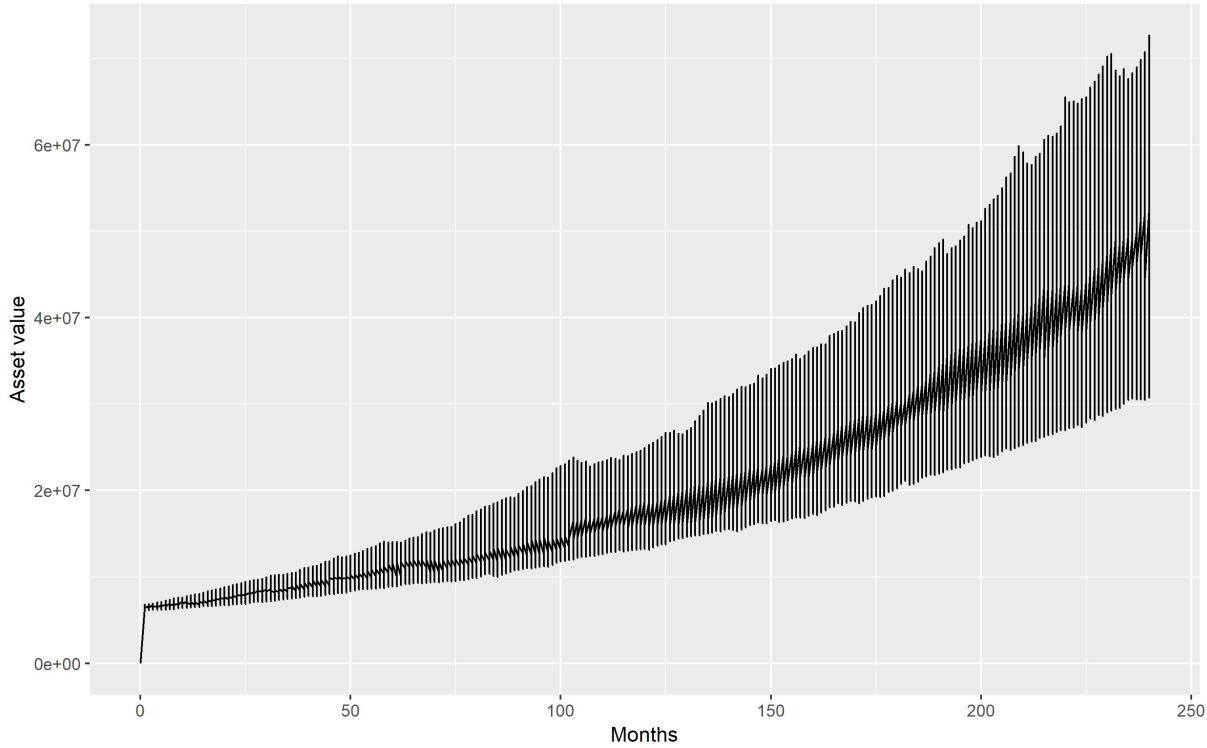

Figure 6-6: Validation assets appreciate / depreciate asset value

6.3.2 Reduce cyber security effectiveness

The main reason organisations need to keep investing in cyber security measures is because cyber security controls becomes less effective over time. There are several reasons explaining why this happens. The discovery of vulnerabilities, new hacker tools, hackers with better skills, etc. all

contribute to the effectiveness reduction of the cyber security controls (Mukhopadhyay et al., 2013). However, depending on the development, the severity of the reduction can differ greatly. For instance, a new vulnerability being discovered has a much larger effect than say a new virus. Therefore, the behaviour of the reduction of cyber security effectiveness should be a chaotic pattern with the occasional peak signifying a larger vulnerability being discovered.

Figure 6-7 shows the graph on the reduction of cyber security effectiveness. This graph uses the same data as figure 6-5, it has an experimentation setup with 432 experiments and 2160 runs in total. The graph seems very chaotic, however when looking at the graph more closely the distinct patterns can be observed. The large number of runs has convoluted the graph but the behaviour of interest is still visible. The expected behaviour was an up and down spiking curve with an occasional peak. This matches the patterns seen in the graph. For the most part there are small and medium spikes observable. But around every 25 ticks there is a large spike observable. Therefore, hereby the model concept of reducing the cyber security effectiveness is validated and will contribute to a more realistic simulation of the cyber security ecosystem.

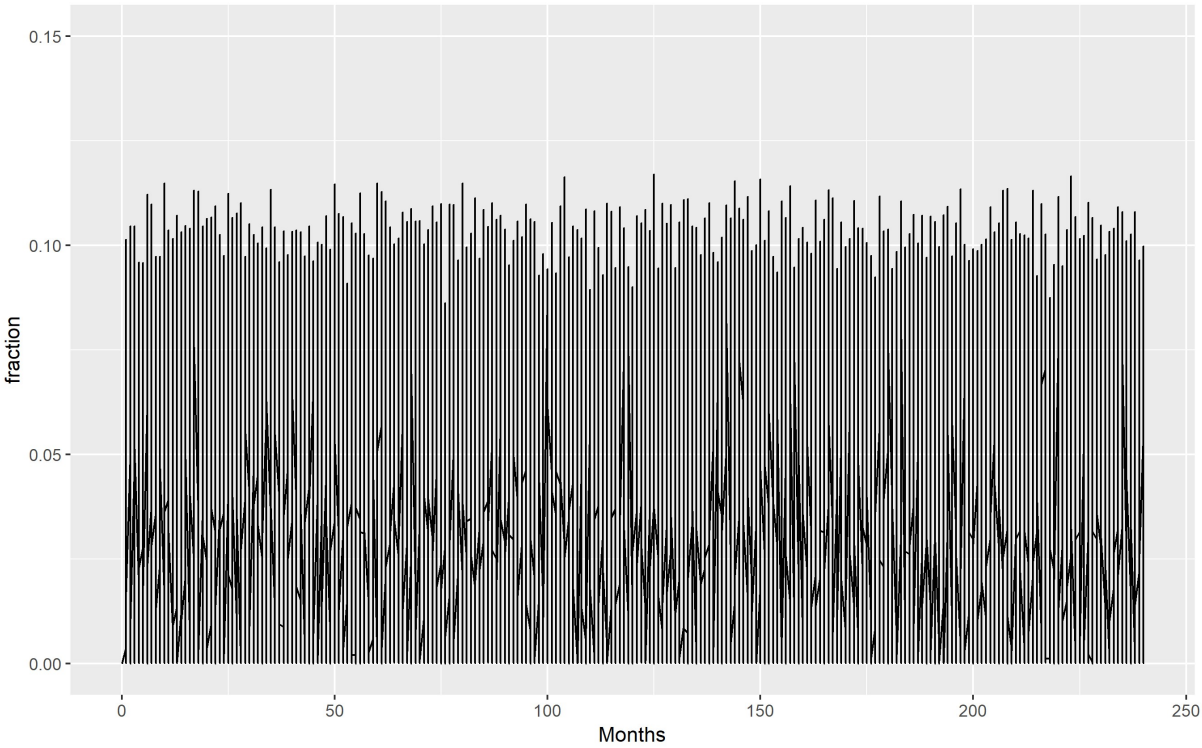

Figure 6-7: Validation reduce cyber security effectiveness

6.3.3 Cyber security investment curve

Organisations invest in their cyber security in order to reduce the risk they face. However, the effectiveness of investments does not show linear behaviour but follows a curve. This means that higher amounts of budget spent actually means a reduced effectiveness depending on the amount (Libicki et al., 2015; Moitra & Konda, 2000). Based on this, the expected behaviour would be to have a relatively steep increase at the beginning which shifts towards a relatively slow increase. In order to model this, a choice was made to define the investment curve as a percentage, thus the upper limit is 1. Since the investment curve is an input variable, it cannot be measured through model runs. However, the input variable itself can be visualised for validation. The formula for the investment curve was presented before in chapter 5 as part of the increase in cyber security strength, for the

validation only the part that defines the curve is necessary. The formula for the investment curve is shown below.

$$y = c_1 - (e \wedge (c_2 \times P)) \quad (9)$$

With:

- y: Effectiveness of the invested amount
- c_1: A constant value set as 1
- c_2: A constant value set as -0.00004
- P: The amount of budget that will be spent

For this validation run, c_2 is of importance since this parameter determines the pattern of the investment curve. For this parameter three values are selected in order to establish the differences between values. The values selected are: -0.0001, -0.00004 and -0.000008, which are differences of -0.00006.

In figure 6-8 the cyber security investment curve is shown. The maximum value for the x-axis has been set to 35000 since this represents a very high investment budget in the model. Thus the figure shows only the investment effectiveness output that is likely to occur in the model.

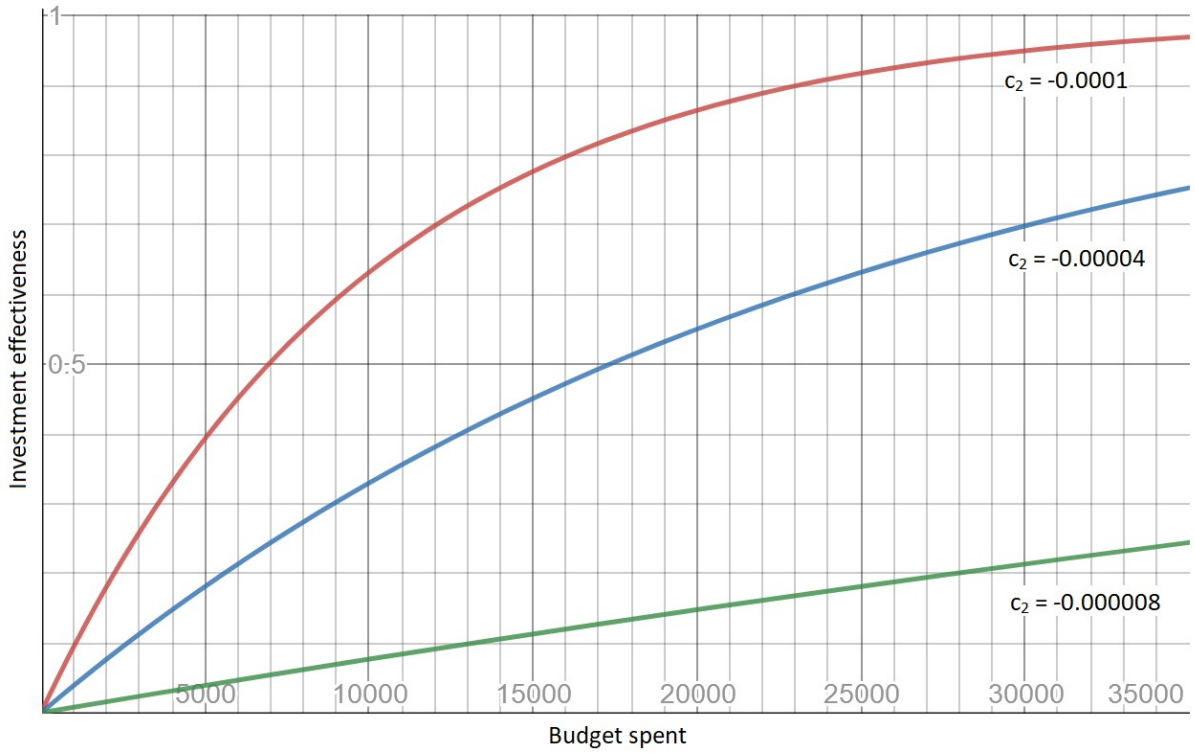

Figure 6-8: Validation cyber security investment curve

Figure 6-8 was made using Desmos graphing tools (Desmos, 2018). Three lines are visible in the graph, the red line represents the parameter value -0.0001, the blue line represents the parameter value -0.00004 and the green line represents the parameter value -0.000008. It was expected that the curve should have a steeper increase in the beginning and shift towards a smaller increase. This is the case for both the red and blue lines. The green line shows more linear behaviour, however, it is likely that if the x-axis showed went beyond 35000, the same pattern would be seen. This means that the exponential function was the correct choice for simulating cyber security investment effectiveness. Looking at the particular values, for an investment of 35000, the red line appears to

come close to a maximum investment effectiveness. It is for this reason that this value was not chosen since it would be rare that an organisation would be able to increase their cyber security to the very limit with one large investment (Libicki et al., 2015). In comparison, the green line is also very unrealistic since, aside from showing linear behaviour, it shows that an investment of 35000 would have 20% effectiveness at most. The blue line shows much more promising effectiveness values. At most an effectiveness of 75% can be reached which seems logical since organisations in the model would rarely be able to spend 35000. Furthermore, the line shows a curve with decreasing effectiveness gains as budget spent becomes higher. Therefore, the logical choice for the model is to use the value of -0.00004 for the cyber security effectiveness investment curve since this will provide the most valid cyber security investment curve.

6.3.4 Tool frequency, success chance and effectiveness

The tool that an attacker utilises can be a crucial factor to its success, which is why it was important to include in the model. There are many different types of tools that attackers can use, with each of them having different chances of successfully breaching an organisations as well as a different effectiveness on obtaining asset value (Blakely, 2012; Denning, 2000; Verizon, 2018). Furthermore, because cyber security controls evolve, the effectiveness of tools is reduced over time. As such, attackers also create new tools or update old tools in order to still be able to breach the defences of organisations. In the agent-based model the choice was made to have attackers select a tool every time they prepare to attack. This simulates the usage of 'new' tools and thus having the same tool effectiveness and success chance. However, since not every tool is as common, a tool frequency has also been included. It is necessary to validate these variables in order to ensure that realistic behaviour occurs in the system. Unfortunately, there is no concrete data on the exact frequency of tools, their success chance or the effectiveness of tools. There are some reports on the number of attacks conducted with certain tools. However, it is very likely that these reports do not possess all the attacks since many organisations tend to be secretive about cyber-attacks or only report attacks that were successful or had a large impact. However, these reports can still provide some basic information that can be used to validate the values chosen for the model.

The values chosen in the model are the following:

Table 6-6: Tool variables in the ABM model

	Tool 1	Tool 2	Tool 3	Tool 4
Tool frequency	0.8	0.3	0.3	0.125
Tool success chance	0.2	0.35	0.5	0.8
Tool effectiveness	0.1	0.3	0.5	0.7

In table 6-6 the values for all three variables for each tool is shown. The variables are scaled between 0 and 1 since they are used for calculations in the attacker procedure. By using this scale it is possible to balance the variables on the behaviour of the model thus obtaining realistic behaviour. However, the difference between the tools can still be validated. Tool 1 represents the most basic hacking tools like malware or viruses, tool 2 represents attacks similar to DDoS or Brute force attacks, tool 3 represents rarer tools like software vulnerabilities and tool 4 represents the rarest types of tools like zero-day hacks. Only four tools were modelled in order to limit the complexity of attackers and keep the model executable.

When looking at the statistics reported by Passeri (2018), it is clear that malware makes up the largest number of attacks, thus a frequency of 0.8 is in line with what would be expected. Furthermore, Verizon (2018) also mentions malware as a large part of the attacks that organisations have to deal with. For tool 2 there is little data available, Passeri (2018) states that a relatively small number of the breaches were caused by DDoS and Brute-Force attacks. However, these methods can be considered hacking tools for which Verizon (2018) states that they were also a large part of the attacks conducted in 2018. However, if the use of vulnerabilities is considered a part of hacking tools, the report from Passeri (2018) also states that it is a large part. Thus by using 0.3 for both tool 2 and tool 3, these follow similar behaviour that is observed in reality. For tool 4 Passeri (2018) mentions that these are rare but that attacks with zero-day hacks still occur from time to time. Therefore, a value of 0.125 seems reasonable to simulate the rarity of this tool.

The success chance of each tool can be derived from the ease of use of a tool and how often it shows up. Verizon (2018) states that there were quite some breaches caused by malware. However, malware is easily accessible and is usually spread without specific targeting (Verizon, 2018). Thus the success rate of it is actually small and a value of 0.2 is actually quite reasonable. DDoS and Brute force are also more automated processes, these can be performed with some ease as long as the attacker has the proper resources available. However, because these tools are more automated, countermeasures have been created as well, decreasing its success chance. A value of 0.35 seems reasonable since DDoS and Brute force attacks are more focussed on a single target, thus the success chance is higher than that of tool 1. Tool 3 involves the usage of vulnerabilities which are actually rarer to find but also provide much better success chances since it exploits unprotected parts of software. However, whilst it can exploit unprotected software it can still be detected, thus a value of 0.5 is logical. Tool 4 refers to the rarest of tools with high success chances. This is because these tools make use of core vulnerabilities in software which cannot easily be defended against. Therefore, a success chance of 0.8 is very logical because organisations will have a hard time preventing and detecting these vulnerabilities.

The effectiveness of tools closely follows the explanation for the success chance of tools but also involves the possibility that the tool provides. For instance, malware can be used to gain access to someone's account, but this usually does not mean that the attacker can steal much. As such tool 1 is in most cases not very effective, whereas gaining access through tool 2 (DDoS/Brute force) will be more effective at stealing asset value. Tool 3 and 4 have an even higher effectiveness since these tools make use of exploits that give much more access to the network of an organisation which allows the attacker to steal more asset value.

The values of the variables mentioned in table 6-6 have been explained and linked to literature. These values can be deemed valid since they follow the history mentioned in literature or because they have been reasoned from their functioning, usage and effects. Thus, by using these values it should be possible to simulate the cyber security ecosystem with some degree of realism.

7. Experimentation results

In the previous chapter, the experimental design was discussed. In this chapter the results from these experiments will be displayed and discussed. This is also the final step of the modelling cycle, the data analysis as defined by Van Dam, Nikolic, & Lukszo (2013).

In this chapter the answers to the following sub questions will be provided.

3. *In the modelled system of organisations and attackers, how does the system react to various policy setups employed by insurance firms?*
4. *What insurance policies can be designed to lower damages across the ecosystem?*

Experimentation was performed with baseline values for general system parameters and varying values for seven experimentation parameters. For specifics of the variables see chapter 6. The experiments have been performed according to a full factorial approach. By performing the experiment like this, it becomes possible to obtain data on possible synergies between experiments. This is because the full factorial approach entails experimenting with all possible combinations of experimentation parameters. Useful insights and results can be obtained through this approach because experimentation parameters might have a small effect on its own but could provide interesting results when combined with other parameters. The experiments have been repeated 25 times in order to reduce chaos and obtain reliable data for analysis. Performing more repetitions would be ideal as this can further decrease uncertainty through chaos and increase the reliability of the data. However, the downside of the full factorial approach is that it is computationally very tasking. Therefore, only a limited number of repetitions were possible.

Similar to the sensitivity analysis, the data obtained from the model has been processed using R (R Core, 2018). For visualisation of the data ggplot2 was used (Wickham & Chang, 2008). R was selected since it is a powerful data analysis tool with much support and its capabilities can be expanded through various packages. This makes it ideal to analyse and visualise the large dataset obtained from experimentation.

The experimentation results will be discussed in two parts. First the individual effects of the insurance options (experimentation parameters) will be described. Analysing the individual effects provides insight into the effect of every option on its own. Therefore, in order to prevent any effect from the other options, the baseline configuration is used with all other experimentation parameters using a value that doesn't affect the system. However, the insurance packages and contract length always influence the system, for these parameters a value was chosen and kept consistent for the individual analysis. The insurance packages were set at the middle value and the contract length at 12 months. The second part of the analysis will focus on the synergetic effects of the insurance policy options. For this part all data has been used to identify if and how combinations of insurance policy options can influence or reinforce their effects in the system.

7.1 Individual insurer policy experiment analysis

The main focus of this thesis is to understand how each insurer policy option influences the system behaviour. In order to analyse the performance of each experiment, the metrics that were discussed in chapter 4 will be used. Specifically, the cyber security strength of organisations and the asset loss that organisations incur will be used to analyse that data since these metrics are the most useful for measuring the influence of each experiment. First the performance of the experiments on the cyber

security strength will be described. This will be followed by a description on the value loss in general and for the insured and uninsured organisations. The metric for the number of organisations that are insured is included for each part of the analysis since the effects of the experiments can only be observed properly when organisations are insured. Moreover, the number of insured organisations can explain why certain behaviour is observed. In each graph the mean will be shown along with 95% confidence bands. The confidence bands indicate how much spread there has been, thus if they are not visible it means that more than 95% of the runs followed the same pattern.

7.1.1 Influence of insurance options on the cyber security strength

The cyber security strength of organisations determines how vulnerable they are to attacks. Thus, for an insurance firm having the cyber security strength of an organisation as high as possible is ideal. However, because of the way insurance works, there is a possibility that cyber insurance actually lowers the cyber security strength of an organisation. This is because it mitigates risk without requiring an investment into cyber security controls. Therefore, it is useful to analyse the influence the experiments have on this metric.

Experiment: insurance package options

The first experiment that will be analysed involves the insurance package options. The insurance package options are combinations of three values for both the insurance premium and insurance coverage as was described in chapter 6. For the insurance packages it was expected that it would have a considerate influence on the system, since organisations make decisions based on the price and the coverage that they provide. In figure 7-1 the cyber security strength and number of insured organisation is shown. In this figure the graphs have been produced for the three insurance package options. Package option 0 is a package that has relatively low values, package 1 has medium values and package 2 has high values. The specifics of the insurance package options can be found in chapter 6. In the figure, a colour has been assigned to each insurance package which corresponds with the same colour line in each graph. The lines that have been drawn in each figure represent the mean value of all the runs of each respective option.

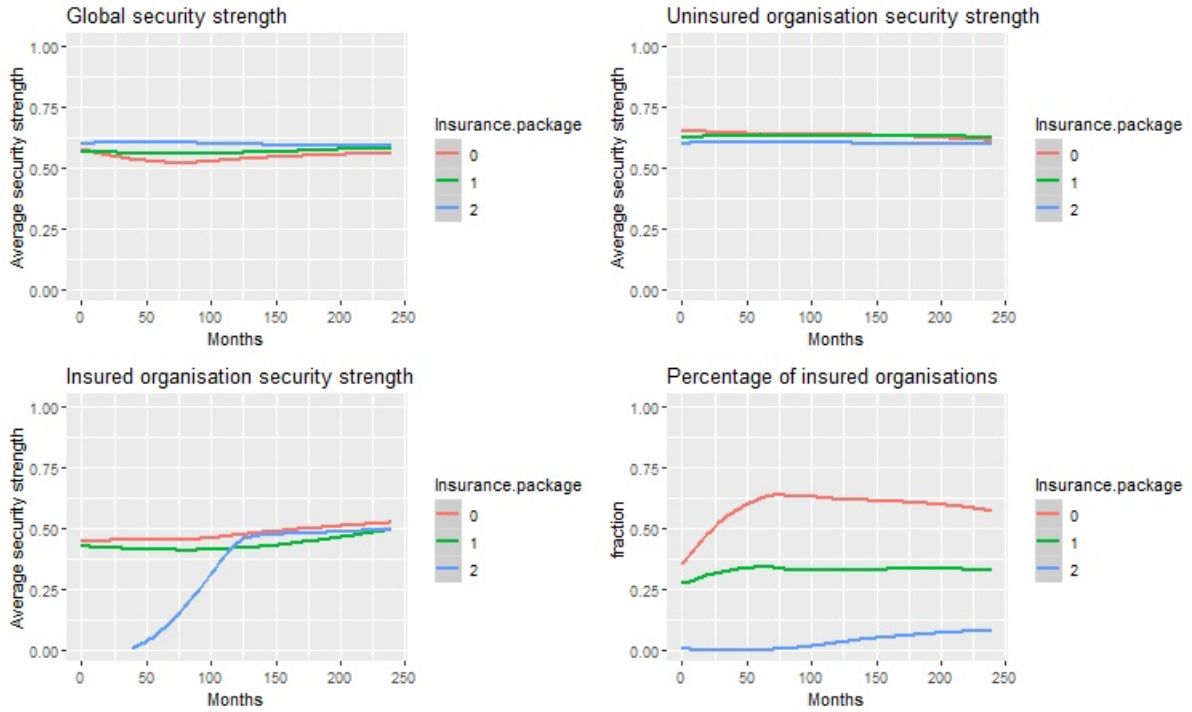

Figure 7-1: Influence of insurance package options on the cyber security strength

The influences of the insurance packages are much closer to each other than expected when it comes to cyber security strength. This goes for the global security strength but also for the uninsured and insured organisation strength. However, when looking at the number of insured organisations there are large differences observable. The influence of an insurance package on the security strength can be explained by looking at the actual parameters that are influenced by it. The insurance packages only affect organisations in their CRM process, making insurance more or less favourable to an organisation depending on the price and coverage. By buying insurance, a part of the available budget is used up and if this makes the risk acceptable they will also stop investing. Furthermore, since insurance mitigates risk without increasing their cyber security strength, it is logical that that option with the most insurance users (package 0) has the lowest average security strength. However, whilst this behaviour is logical and seems realistic, it could be influenced by modelling choices that were made to simulate the system. In the model, organisations are fully rational and stop investing when they reach an acceptable risk. Whereas in the real system, additional variables like wanting to protect their image or valuing intellectual property might drive an organisation to keep investing. However, whilst option 0 has the lowest average security strength, it also has the highest security strength for insured organisations. This is because the prices are lower for package 0 thus more funds are available for investments. Additionally, because the prices and coverage are lower, the package is likely a better fit to the amount of asset value at risk and becomes an addition to their cyber security investments instead of the sole solution to mitigate it. With an increase in insurance price, there is a visible drop in the number of organisations that opt to buy insurance. This is logical since the price for investments into cyber security controls end up being cheaper to reduce risk compared to buying insurance. Although, here too modelling choices could be a factor since the choice for buying insurance rests solely on the coverage and price. One last interesting result is that the average cyber security strength is higher if fewer organisations buy insurance. This is to be expected since buying insurance leaves fewer budgets available to increase cyber security strength. Furthermore, insurance

can drop the risk for organisations to acceptable levels meaning they will be satisfied with their current cyber security level and stop investing.

Experiment: contract length

3 values were chosen for the experiment with the contract length: 6, 12 and 24 months. The 3 values are represented by their own colour in each graph shown in figure 7-2. The contract length was not expected to amount to much on its own but rather through synergies with other options. However, it is still useful to establish what behaviour is brought forth through varying the contract length by itself.

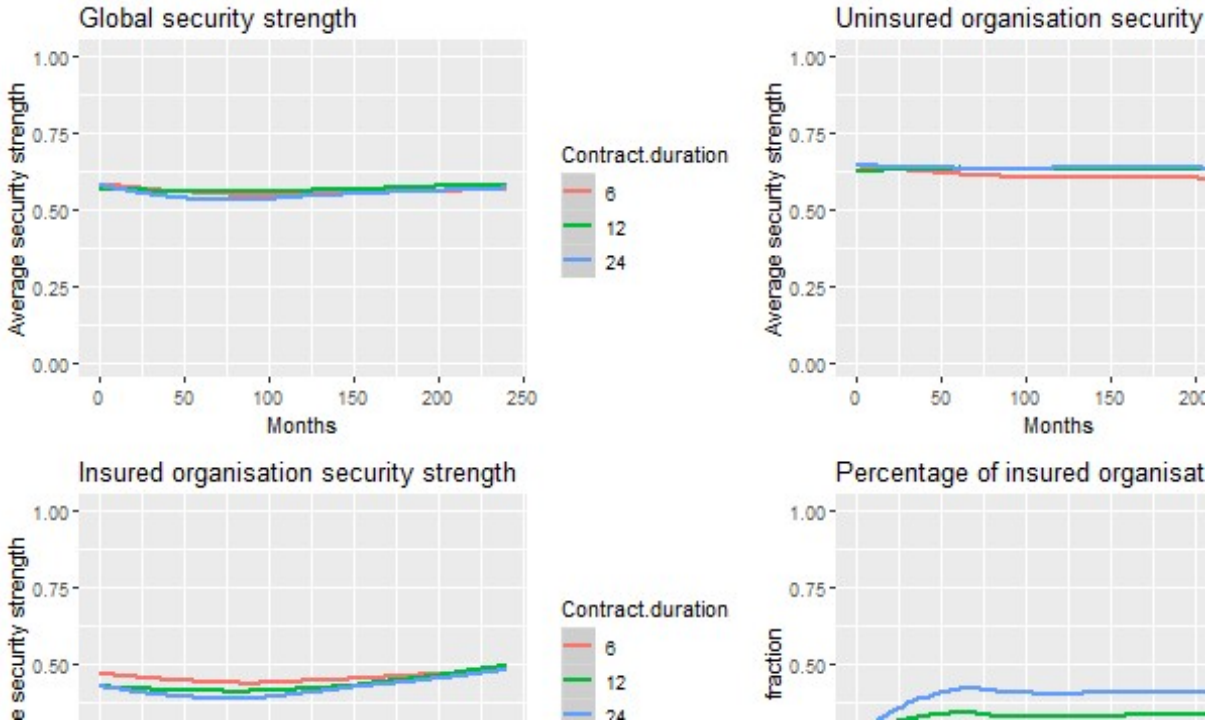

Figure 7-2: Influence of contract length on the cyber security strength

As can be seen in figure 7-2, the contract length has very little effect on the cyber security strength. Every line drawn for each contract length value ends near each other. There is a slight difference visible in the uninsured organisation security strength, where the contract length of 6 months ends up lower. However, this is a result of the number of insured organisations being reduced slightly towards the end of the run. Since they had cyber insurance, their cyber security strength was a bit lower. This amount got added to the uninsured cyber security strength towards the end. The only real difference visible in figure 7-2 is in the graph for the number of insured organisations. In this graph it quickly becomes apparent that for longer contract durations the number of organisations is higher and has a more constant run towards the end. This behaviour can be explained by the consequences a contract has for organisations. The contract binds the organisation to their decision to obtain insurance for the duration of the contract. This means that they will have to keep making payments until it ends. As a result, the organisations have a reduced budget available to invest in cyber security controls. This causes organisations to either lower their investments because they run out of budget or because they choose to stop investing because risk is already acceptable. Thus when the budget ends, it is once again the best option to reduce their risk and they renew it. However, this influence could also be influenced by model behaviour. This is because in the model the organisations don’t have an opinion on the commitment of a contract. In the real system, it is

possible that organisations would prefer shorter contracts and thus will think again before entering into a long term commitment. Furthermore, the organisations only take a year into account at maximum, since they would have to reserve money till the annual budget allocation. As a result of these model choices, it is possible that the number of organisations that buy insurance would end up lower. However, the stability of the runs would likely stay the same.

Experiment: risk selection

The risk selection experiment involves a risk selection factor that has been varied over three values: 0, 0.25 and 0.5. The risk selection option is used to prevent taking on too much risk by insuring organisations with low security strength. The three values have each been assigned a colour during analysis which makes it possible to discern the performance for each value. It is expected that the risk selection option will reduce the number of insured organisations but as a result will lead to higher cyber security strength for insured organisations.

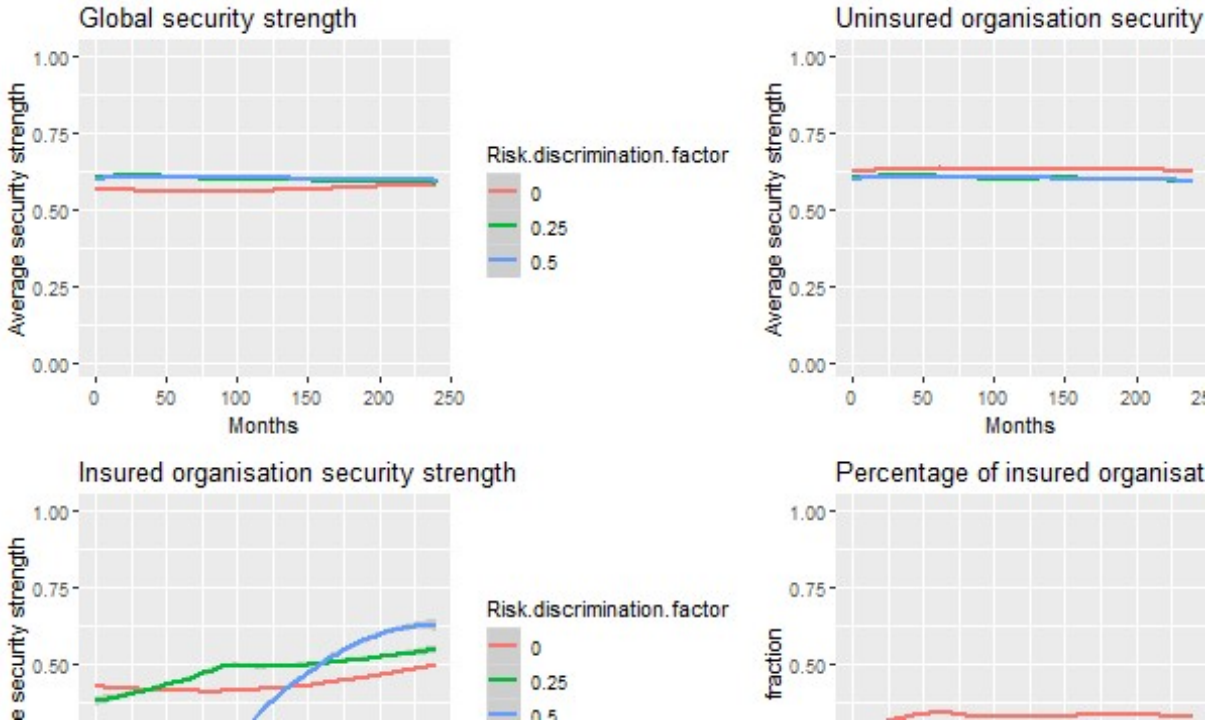

Figure 7-3: Influence of risk selection factors on the cyber security strength

The influence of risk selection is very difficult to see since the performances of the three runs are very similar. The global security strength shows a slightly better performance for a discrimination factor of 0.25 and 0.5. Similarly, the insured organisation security strength shows that insured organisations have a higher cyber security when risk discrimination is active as well. However, this behaviour becomes clear when looking at the number of insured organisations. When risk discrimination is active, there are very few organisations that buy insurance. This is because risk selection makes it too expensive for organisations to obtain insurance with low cyber security strength. Thus, only organisations with a higher cyber security level or a high available budget will be able to obtain insurance. The influence that risk selection has on the system is expected. However, whilst it might seem that it a bad choice for an insurer to apply risk selection, it is important to note that the model has a limited number of organisations. This means that it might still be a good decision for an insurance firm to reduce the risk it takes on, but they would still need to find enough organisations to be viable. However, risk selection is not necessarily beneficial to the system when it

comes to cyber security strength. Risk selection also has a strong correlation with the insurance package used. For example, using insurance packages that have relatively low prices for high coverage, risk selection would not cause a large or unrealistic amount to be asked. Furthermore, organisations with a high cyber security level would likely also apply for insurance since it costs less whilst providing high coverage, as was also mentioned in the experiment of insurance packages.

Experiment: incentivisation

The experiment for incentivisation was done using a true and false value. True means that the option is on and that the organisations are incentivised to invest in their own cyber security, whilst false simulates a baseline situation. In the graphs two colours are used to indicate both values. It is expected that organisations will continue increasing their cyber security when insured. Incentivisation will also prevent a moral hazard from occurring.

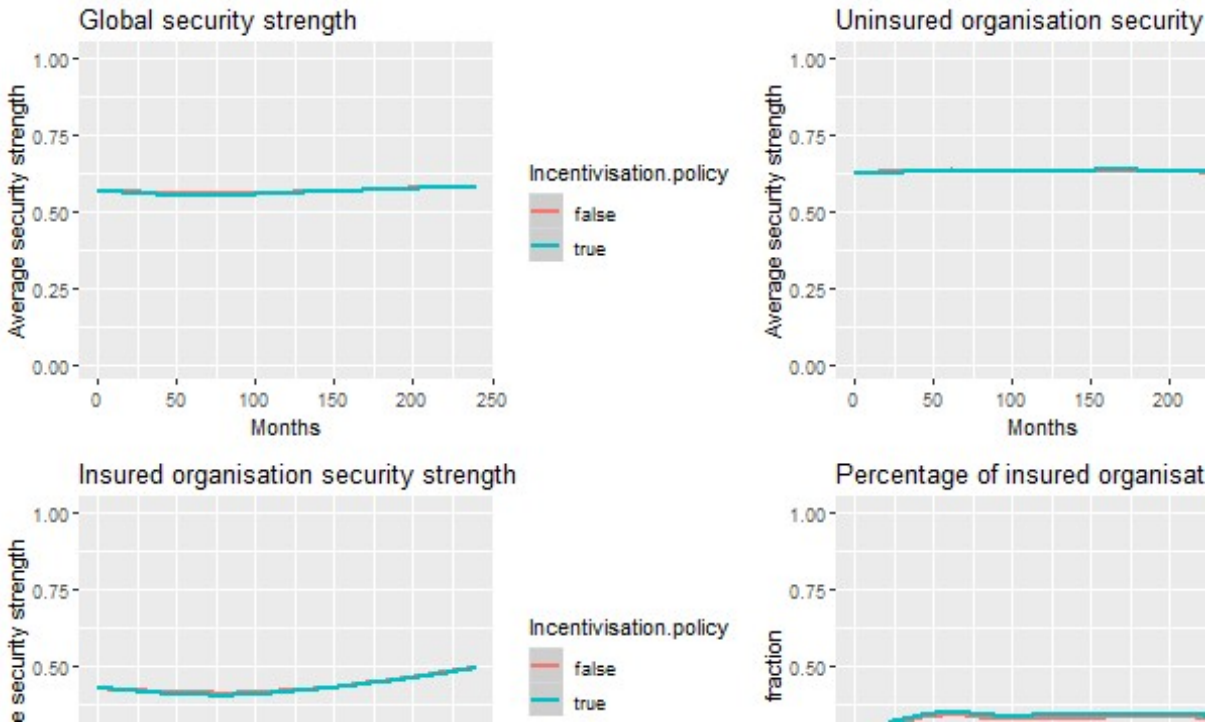

Figure 7-4: Influence of incentivisation on the cyber security strength

Figure 7-4 shows very little difference between the two incentivisation options. All the graphs show that both values have the same pattern. This is quite unexpected since every organisation that has an acceptable risk or would make a smaller investment or at least invest the budget to achieve the incentivisation amount. This is also a model choice, since the organisations will always invest enough to obtain the benefits of the incentivisation policy. However, the behaviour in figure 7-4 would state that each organisation already invested more than the incentivisation budget, which is why there is no difference between the two values. An artefact of the model that could be influencing the performance is that organisations don't take into account the discount on their premium price, they will only try to obtain it when they have enough budget. Furthermore, in the model to obtain the benefits of the incentivisation policy in the model, organisations have to invest a percentage of their budget. In the actual system, incentivisation is focussed at specific controls that organisations would have to implement. Additionally, in the model, the incentivisation benefit of an organisation is also not remembered when obtaining a new contract. Thus, organisations can only enjoy the benefits for the length of the contract. In order to increase the effects, it could be possible to increase the

amount of budget that has to be spent. This would likely have the largest effect on the performance since it would make organisations spend more on cyber security if they want to fulfil requirements for incentivisation. Changing the premium reduction for incentivisation would provide a small effect since its effect in the current model would only be that organisations have more money available after fulfilling requirements.

Experiment: upfront risk assessment

Similar to the incentivisation experiment, the upfront risk assessment is also performed through a true and false value. True meaning that the option is active and false simulating the baseline situation. Once again the graphs have given the two values a colour making it possible to discern the performance. For the upfront risk assessment the expectations are that organisations were that organisations do not opt for insurance since it would cost more than just the premium. However, was also expected that it would have a positive effect on the cyber security strength of insured organisations.

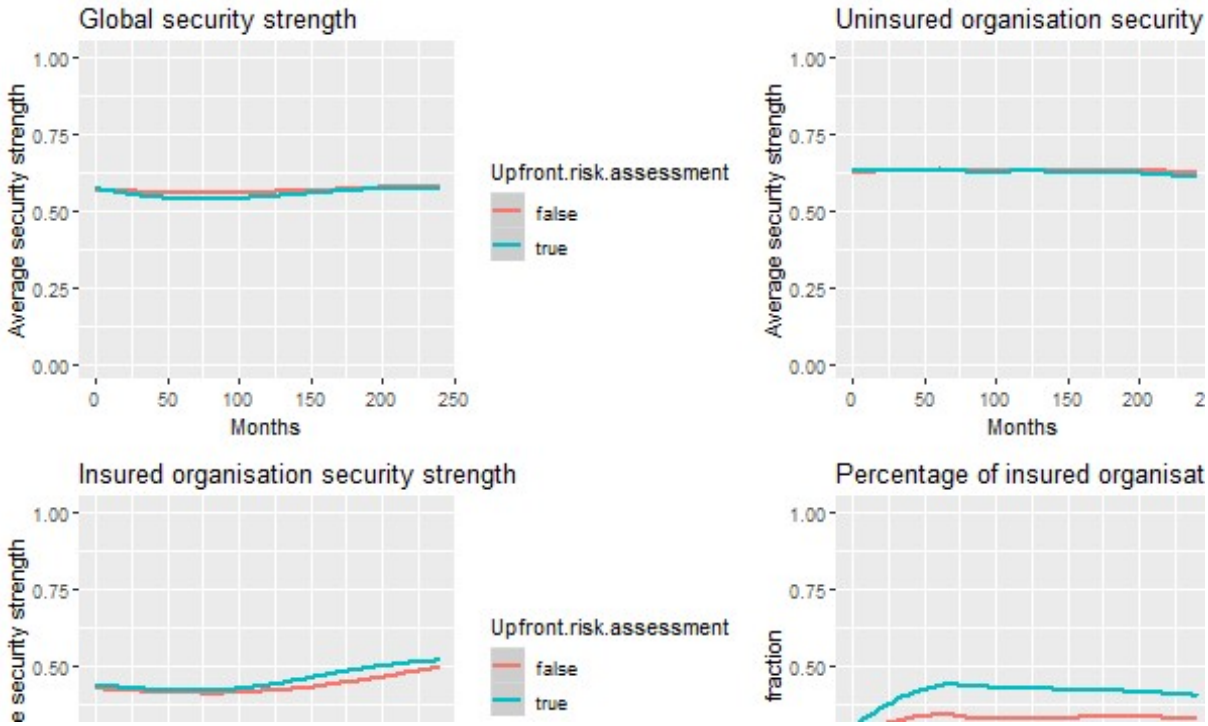

Figure 7-5: Influence of upfront risk assessment on the cyber security strength

The first thing to mention about this graph is that there is a slight advantage to the security strength for insured organisations when the upfront risk assessment is used. Furthermore, against expectations, more organisations choose to buy insurance compared to the baseline. The positive effect on the insured organisation security strength was expected and can be explained. The assessment is performed by the insurance firm and helps organisations to identify vulnerabilities. Therefore, the first investment done by the organisation will be more effective because the organisation knows what vulnerabilities it needs to cover. Part of this behaviour could be caused by model decisions. In the model, the organisation assesses the investment benefit it would have if upfront risk assessment is active. In the actual system, organisations would not know how much benefit they would have from the risk assessment. Thus it could be possible that an organisation would determine the best option equal to the baseline despite the possibility of an investment benefit. In order to increase the effects of risk assessment, the benefits obtained from it should be

higher. This is a difficult thing to do since it means that an insurance firm should possess and provide data with a much higher quality (e.g. more detailed information on vulnerabilities and effectiveness of controls). This would help organisations to make the best investments in their cyber security with the lowest amount of money. Therefore, despite having less money because of buying insurance, the cyber security strength could still end up higher compared to not buying insurance.

Experiment: sharing cyber security control information

A true and false value was used to perform the experiment for sharing cyber security control information. The true value enables the sharing of data whilst false disables it and thus simulates the baseline scenario. In figure 7-6 the graphs to analyse the influence of sharing data is shown. In the figure the values true and false can be discerned by their colour. It is expected that sharing cyber security control information will affect the system similarly to the upfront risk assessment. However, it will be more effective since it doesn't cost anything extra and stays in effect as long as an organisation is contracted.

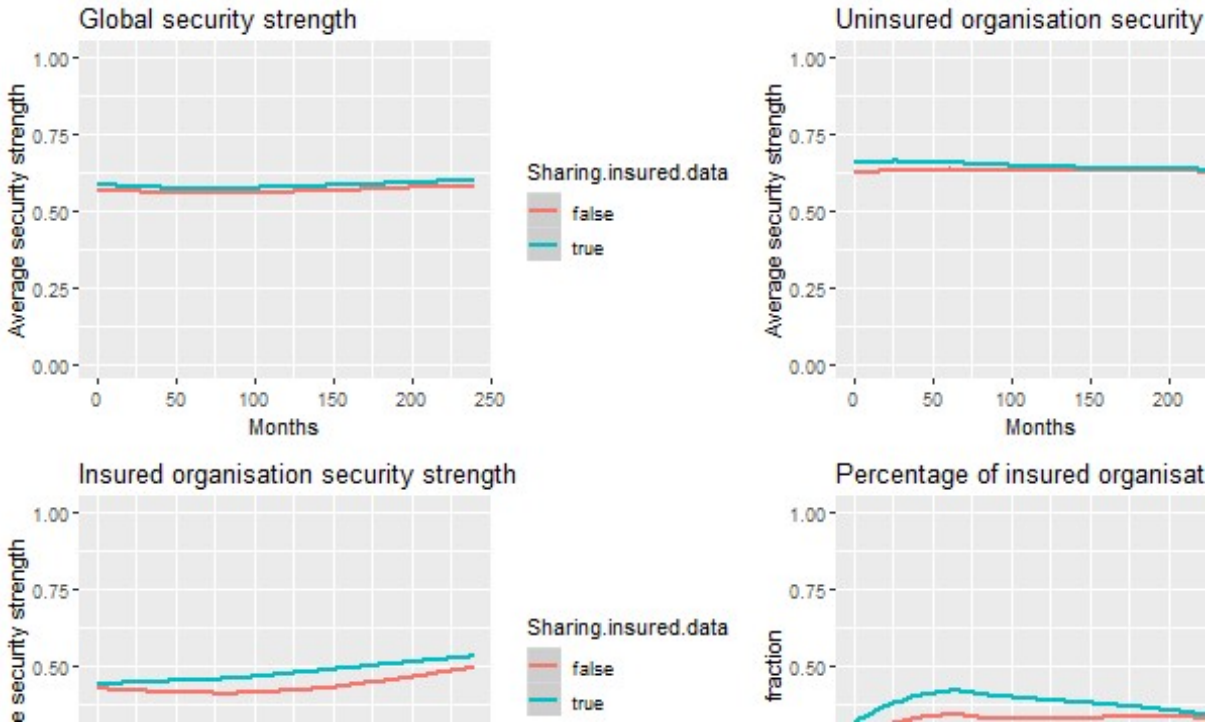

Figure 7-6: Influence of sharing cyber security control data on the cyber security strength

Looking at figure 7-6, there is very little effect observable when looking at the global security strength and uninsured organisation security strength. However, looking at the insured organisations security strength, a slight difference can be seen. This difference is similar to how the upfront risk assessment influenced the system. However, it seems that the cyber security strength of this experiment rises slightly steeper. The reason behind this would be that sharing cyber security control data is always active when an organisation is contracted whilst the upfront risk assessment benefit is only received when making a new contract. Similar to the upfront risk assessment, the effects of sharing cyber security control data can be influenced by model decisions. Like the upfront risk assessment, the organisation is able to take into account the benefit from the shared data. However, this is not necessarily unrealistic for this experiment since the organisation would receive the information before decisions are made. However, the effect of sharing the data is always the same in the model. This would not be the case in the actual ecosystem since it would depend on what kind of

information is obtained and the quality of the data. This could reduce the rate at which the cyber security for insured organisations would increase their cyber security. There is also interesting behaviour observable in the number of insured organisations. The number of insured organisations is reduced towards the end of the run. The only explanation for this would be that the organisations got close to an acceptable risk level at which point investing in security costs less than buying insurance. The same method that was described for the upfront risk assessment applies to sharing insured data when looking at ways to increase the effect of the insurance policy. This is because the effect of this policy also comes forth in the investments of organisations. By providing higher quality data, the effectiveness of investments can be increased, thus offsetting the reduced budget and leading to a higher cyber security level.

Experiment: requiring organisations to maintain their security level

The experiment for maintaining the cyber security level that organisations had when buying insurance is performed with a true and false value for the option. The true value means that the option was active during the run and false that it was off. As such, the false option simulates the baseline scenario. The graphs used for analysis are shown in figure 7-7. In the graphs the runs are discerned from each other through colour coding. Requiring organisations to maintain their security level can be an effective mechanism against moral hazard. Furthermore, it can give organisations a minimum level thus making sure that they won't let their security strength fall once they obtain insurance.

Figure 7-7: Influence of requiring organisations to maintain security level on the cyber security strength

In contrast with the expectations, there is nearly no difference observable between the use of a mandatory security level and the baseline without it. None of the graphs show any difference between the two values. The explanation for this can be found in the investments organisations make. It is likely that the organisations are already investing large amounts thus already possess the mandatory level. It is possible that this experiment would show much more promising results if there were organisations at a high cyber security level and thus near an acceptable security level. This

could be more promising since these organisations would then likely drop their cyber security level a bit when obtaining insurance. The effects could also be more pronounced if the coverage of insurance was much higher, since this would lead to insurance covering most if not all of the asset value at stake making the risk acceptable and additional investments unnecessary.

7.1.2 Effects of insurance options on the value loss

The potential value loss that organisations can suffer is the main reason the cyber security ecosystem exists. Organisations conduct CRM processes to assess and try to reduce their risk in order to reduce the potential value loss possible. For the insurer this is also of great importance, since they insure and have to pay out on damages and losses. Therefore, the insurer wants to reduce this amount as much as possible as well. Thus analysing the influence of each experiment on the value loss of organisations can provide very useful insight.

In the previous section most if not all of the artefacts of the model and their influence on the experiment performance has been discussed. Therefore, in this section, only additional or important model decisions will be described. Furthermore, the methods to increase the influence of experiments have also been discussed previously and will not be mentioned in this section.

Experiment: insurance package options

As was mentioned above, the insurance package options include both the insurance premium and coverage. Three package options were designed: package 0, package 1 and package 2. These packages range from low values to high values. In figure 7-8 the data concerning the effect of the packages on the value loss is shown. In the graphs the packages have been given a colour to make discerning them possible. The expectations are that the insurance packages have very little effect on the value loss. This is because the packages only include the premium and coverage, there are no additional effects.

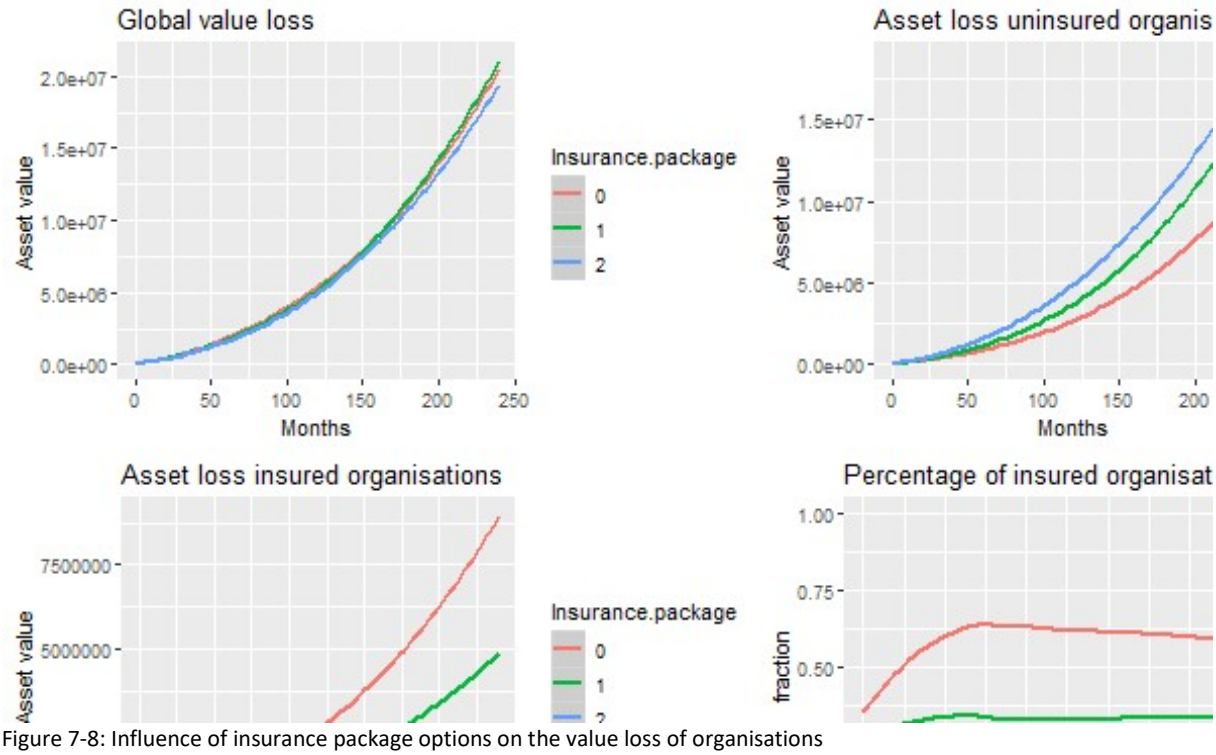

Figure 7-8: Influence of insurance package options on the value loss of organisations

The global value loss shows very little difference between the runs, as was expected. The other graphs do show some differences but these can all be explained by looking at the number of insured organisations. The runs for insurance package 2 show very low asset value loss for insured organisations because there are practically none until around 75 ticks when the numbers start growing. However, insurance package 2 is also the most expensive setup. Therefore, the organisations that buy insurance are likely also the organisations that possess a high budget which allows them to invest in cyber security controls and buy insurance. Therefore, it can be concluded that the insurance package options nearly no influence on the value loss of organisations.

Experiment: contract length

The contract length has three values that are used to experiment with these parameters. The values are 6, 12 and 24 months. These values have been represented through colours in the data analysis figure below. It is expected that the contract length has very limited influence on the amounts of value loss. This is because, similarly to the insurance packages, this parameter only influences the system through the contract length and contains no specific drivers for improving cyber security.

Figure 7-9: Influence of the contract length on the value loss of organisations

In figure 7-9 it can be seen that there is actually very little effect of the contract length on the value loss experienced by organisations. This is because the asset loss of insured organisations is actually following the pattern of the number of insured organisations. With more organisations the asset loss is higher since there are more organisations incurring attacks. Whilst with fewer insured organisations there is less asset loss since only a few organisations are attacked. However, there are a few differences visible. In the global value loss, a contract length of 6 months seems to lower the value loss by a bit. This can be explained by the effect the contract has on the acquisition of insurance. As can be seen in the graph for the number of insured organisations, the number of insured organisations goes down as the contract duration becomes shorter. This behaviour occurs because organisations can drop their contract sooner when it is better to invest in their own cyber security. As was mentioned before, insurance displaces risk but does not increase the control

strength. Therefore, the more uninsured organisations there are the higher the overall security strength and thus the lower the losses. This is the reason why this behaviour is only observable in the graph for the global value loss.

Experiment: risk selection

The values used for risk selection are 0, 0.25 and 0.5. These values have been colour coded in the analyses in order to be able to discern between the runs. It is expected that risk selection can have an effect on the value loss of insured organisations. This is because the insured organisations will only be able to afford insurance once they manage to obtain a decent cyber security level or when they have a high enough budget. Figure 7-10 shows the data analyses for the influence of risk selection on the value loss.

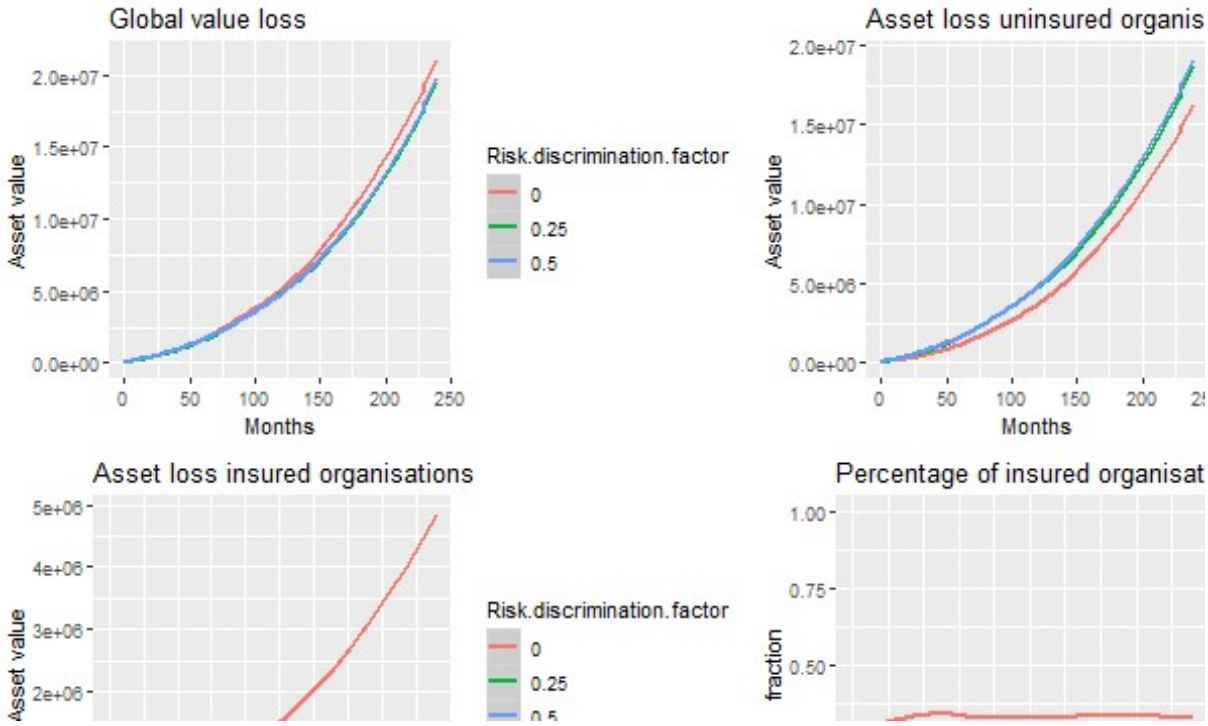

Figure 7-10: Influence of risk selection on the value loss of organisations

Looking at figure 7-10, it seems like the expectations were correct. The value loss is lower whenever the insurance firm discriminates organisations based on their cyber security level. For both values, the asset loss for insured organisations is very low. However, for both values, there are also very few organisations that are insured. Furthermore, the effect of risk selection can also be seen in the graph for the global value loss. When risk selection is used, there is a slight decrease in global value loss. It is possible that the model decisions are of influence on the performance of risk selection. In the model the organisations are completely rational and do not look ahead towards better possibilities. This means that an organisation will not strategize in order to increase its security level and buy insurance against a cheaper price. If this was possible, there might be more organisations that would attempt to obtain insurance which could change the behaviour.

Experiment: incentivisation

Incentivisation is used to motivate organisation to invest a minimum amount into security controls. For this parameter two values are used: true and false. For the incentivisation the expectation is that it can have a large effect on the value loss since it would keep organisations investing in their

security. However, as was seen in the analysis of the effect of incentivisation on the cyber security of organisations, the main problem is that most organisations already invest a large amount of their budget. Thus it is very likely that there will be little effect on the value loss.

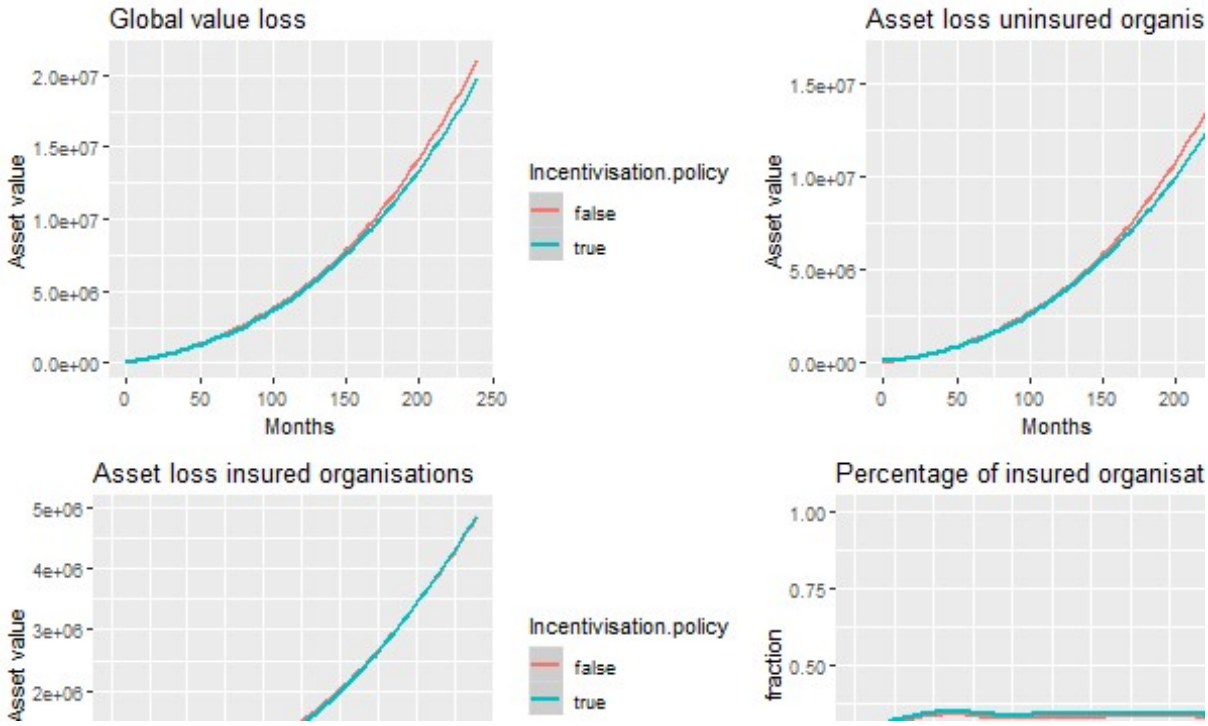

Figure 7-11: Influence of incentivisation on the value loss of organisations

The analysis of the effect of incentivisation shows that there is very little effect noticeable. However, the small differences that are visible show that the expectations are correct, albeit in a slightly different way. With incentivisation active, there is a small decrease in global value loss visible. This same pattern is observable in the graph for uninsured organisations. However, the graph for asset loss of insured organisations does not show this behaviour. Therefore, the reason for the small decrease in value loss can be found in the number of organisations. It seems that, because of incentivisation, more money is available allowing organisations to balance themselves better between being insured and investing in cyber security. As a result, there are more organisations insured. Furthermore, despite the slightly increasing number of insured organisations, the value loss for insured organisations is the same as the baseline situation. This means that, incentivisation did have an effect but that it is very small. The modelling choices also play a role for this parameter. This is because the model does not allow for organisations to strategize and take advantage of renewing contracts. This could make a difference and make the positive effect more pronounced. For example, an organisation in the ecosystem could obtain insurance with the idea of taking advantage of incentivisation. This could lead the organisation to pay relatively little for insurance and have more budget available for investments in controls.

Experiment: upfront risk assessment

The values false and true are used to experiment with the upfront risk assessment. In figure 7-12 the graphs of the upfront risk assessment are shown, in these graphs the true and false value runs have been colour coded. The upfront risk assessment is used to assess the risk the insurer takes on by insuring an organisation. This provides the insurance firm with information on the cyber security of the organisations and allows them to advise organisations on vulnerabilities. This makes

organisations invest their budget more effectively when they obtain a new contract. Therefore, the expectations are that it will lower the value losses for insured organisations.

Figure 7-12: Influence of an upfront risk assessment on the value loss of organisations

Analysis of the upfront risk assessment shows that the insured organisations are actually attacked more often. However, the higher value can be explained when looking at the number of insured organisations. The graph shows that there is some difference in the number of organisations between the baseline and upfront risk assessment runs. A higher number of insured organisations lead to more value loss, since there are more organisations that can lose value. The global value loss seems more reliable to measure the performance since it does not differentiate between insured and uninsured organisations. In the global value loss graph it can be seen that there is a positive effect. Meaning there is less value lost when upfront risk assessment is used by insurance firms, although the difference is very small.

Experiment: sharing cyber security control information

For the experiment of sharing cyber security control information with insured organisations, the values true and false are used. These two values have also been used to differentiate between runs through colour coding. Sharing cyber security control information means that insurance firms share the information they amass from all clients about controls, vulnerabilities, etc. By sharing this information, the organisations can make more efficient investments in cyber security controls, similar to the upfront risk assessment. However, unlike the upfront risk assessment, sharing is active for an organisation as long as it is contracted. Therefore, it is expected that the effects from sharing security control information will be the same or have more effect compared to the upfront risk assessment.

Figure 7-13: Influence of sharing cyber security control information on the value loss of organisations

The graphs in figure 7-13 suggest that the expected effects were correct. Sharing cyber security control information is indeed more useful to insured organisations compared to the upfront risk assessment experiment. Whilst the number of insured organisations indicates that there are more insured organisations when sharing insured data is true, the asset loss graph for insured organisations state that the asset loss is actually still lower than the baseline run. However, when looking at the global value loss, the effect is less obvious but still there. The rapid decrease that is observable in the graph for the number of insured organisations can be explained by the reasoning to obtain insurance. Insurance is only useful if it allows organisations to mitigate the risk with a lower investment. It is likely that the influence of sharing data allows organisations to reduce their risk to nearly acceptable values, at which point, investing in their controls is cheaper than buying insurance.

Experiment: requiring organisations to maintain their security level

In the experiment that requires organisations to maintain their security level, the value true and false have been used. These values are also shown in the graph and have been given a colour to make discerning the runs possible. For this experiment the expectations are that it will make sure that the cyber security of insured organisations stays the same and will keep rising as time progresses. However, there is also a chance that it will have no effect at all since organisations have to invest considerate amounts in order to mitigate risk. Therefore, the regular investments can be high enough to always keep the security level stable thus preventing the effects of the option from kicking in.

Figure 7-14: Influence of requiring organisations to maintain security level on the value loss of organisations

Figure 7-14 contains the graphs that can be used for analysis of the effect or a mandatory security level. Interestingly, the global value loss and asset loss for uninsured organisations show a slight difference between the two values. The run that required a mandatory security level ends up losing less value in both runs. This behaviour is even smaller for the insured organisation asset loss. In the middle of the run, a very small difference is visible. The results obtained for this experiment could partly be caused by model decisions. This is because in the model, organisations have no opinion on the mandatory increase that is required. As a result, organisations will buy insurance and always try to fulfil the mandatory security level condition.

7.2 Synergy experiment analysis

In the previous section the individual influence of each experimentation parameter was discussed. In this section the focus is on analysing synergetic effects between insurance options if these exist. However, based on the previous chapter, it has already become apparent that not every insurance option will be able to create synergetic effects. For instance, risk selection greatly reduced the number of insured organisations and does not necessarily improve the security or value loss in the system. Therefore, not every possible combination will be discussed, instead several potential parameters have been selected and will be discussed below.

7.2.1 Synergy experiment setup

The parameters that have been selected to analyse synergetic effects are: contract length, sharing insured data, incentivisation, and required security level. These parameters showed promise because they had a positive effect compared to the baseline. The contract length showed that for a shorter contract, whilst there are fewer organisations insured, the global losses go down. Furthermore, the losses for insured organisations seem to go down as well. Sharing insured data was selected because in the analysis for the cyber security level and for the asset loss it showed positive effects. It is also similar to the upfront risk assessment which showed very similar results. It is thus also not necessary

to include both parameters. On the first look at the results for incentivisation, there seems to be nearly no effect. However, analysing the graph actually shows that there is a slight effect since more organisations can be insured and the amount that was lost stayed the same. Furthermore, it reduced the global value loss in the system. The required security level option is very similar to the incentivisation option. There is little to no effect visible when considering the cyber security strength but when analysing the value losses a difference can be discerned. The effect is the same as the incentivisation option in that the global value loss is reduced through it.

These experiments all showed very little influence on the metrics used to measure their performance. However, there is a possibility that combining some of these options might lead to more discernible effects or give insight into the limitations of insurance policies.

In order to perform experiments for synergy, the values for each experiment parameter that provide the best performance need to be identified. After the most promising setup has been determined, the performance of the runs can be compared to the baseline which was also used for the individual analysis shown above. Since it is not possible to analyse the effects of all parameters at the same time, it is necessary to analyse the effect of parameters based on their experimentation values. This will allow for the selection of a value for these parameters thus reducing the number of dimensions that need to be analysed.

7.2.2 Analysis of synergetic parameters

For the first step the parameters selected are: contract length and required security level. These parameters have been setup in a grid, showing the respective runs for each value of these parameters. Furthermore, the other parameters have been added into each figure. The values for the other parameters can be discerned by colour. Below figures 7-15 – 7-18 are shown, each figure contains multiple facets showing the possible combinations of parameter values. The figure 7-15 and 7-16 show the influence of the parameters on the cyber security of insured organisations and figure 7-17 and 7-18 show the effect on the value loss of insured organisations. The rows indicate whether the required security level option is active or not, whilst the columns indicate which contract length is used.

As can be seen in the figure 7-15 and 7-16, very little difference is visible between the rows. This means that the required security level has had very little influence on the cyber security level of insured organisations. Figure 7-17 and 7-18 show slightly more discernible effects between the values of required security level. This is especially the case when looking at a contract length of 24 months. The value loss in both figures ends up lower when there is a required security level. The contract length shows more discernible differences between each value. Whilst, figure 7-15, where the incentivisation effect is added as parameter, shows little effect for different contract lengths, figure 7-16 shows slightly more visible differences. When looking at the value lost by insured organisations the effect of contract length can be observed quite precisely. For longer contracts the value loss seems to become lower. However, the number of users for insurance is higher with a longer contract as was shown in figure 7-2 that is part of the individual experiment analysis. This does not have to be problematic since the synergy between the parameters is of interest in this experiment. Furthermore, for an insurance firm it is likely to be more ideal to have more clients. Therefore, using a contract length of 24 months seems to be the most optimal value for contract length. However, when looking at figure 7-16, the effect of sharing control data appears to be more

visible with a shorter contract. This is in contrast with figure 7-18 where the value loss is lower when a contract of 24 months is used in combination with sharing control data and requiring the security level to be maintained. However, figure 7-18 might make it seem larger since there are more organisations insured thus the effect becomes more pronounced. The incentivisation policy shows positive effects as well when the contract length is 24 months. The effects are largest when looking at the value loss of insured organisations but could be showing this performance for the same reason as sharing the insured data. Therefore, it is not exactly clear how large the value for contract length should be as each parameter seems to be influenced by it in a slightly different way. As such, using all values of the contract length for synergy experimentation might provide more insight.

The values selected for the synergy experiment are the following:

- Contract length: 6 - 24
- Required security level: true
- Incentivisation: true
- Sharing control data: true

Using these values provides a promising setup that can provide the positive effect on the ecosystem. However, it is necessary to mention that these results could be artefacts of the agent-based model. These artefacts were discussed during the individual experiment analysis and apply to the results in this section as well. However, the synergy experiment is still useful to obtain insight into the effects that can be achieved by combining several options.

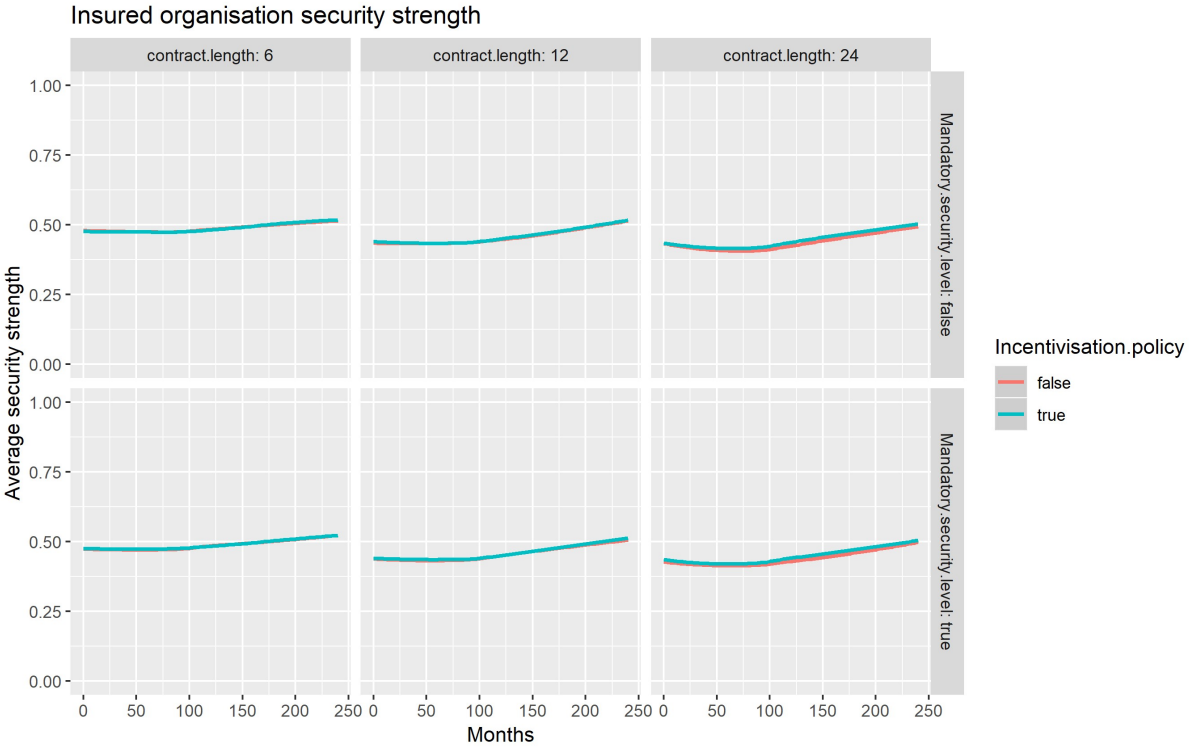

Figure 7-15: Facets on the influence of contract length, required security level and incentivisation on the cyber security level of insured organisations

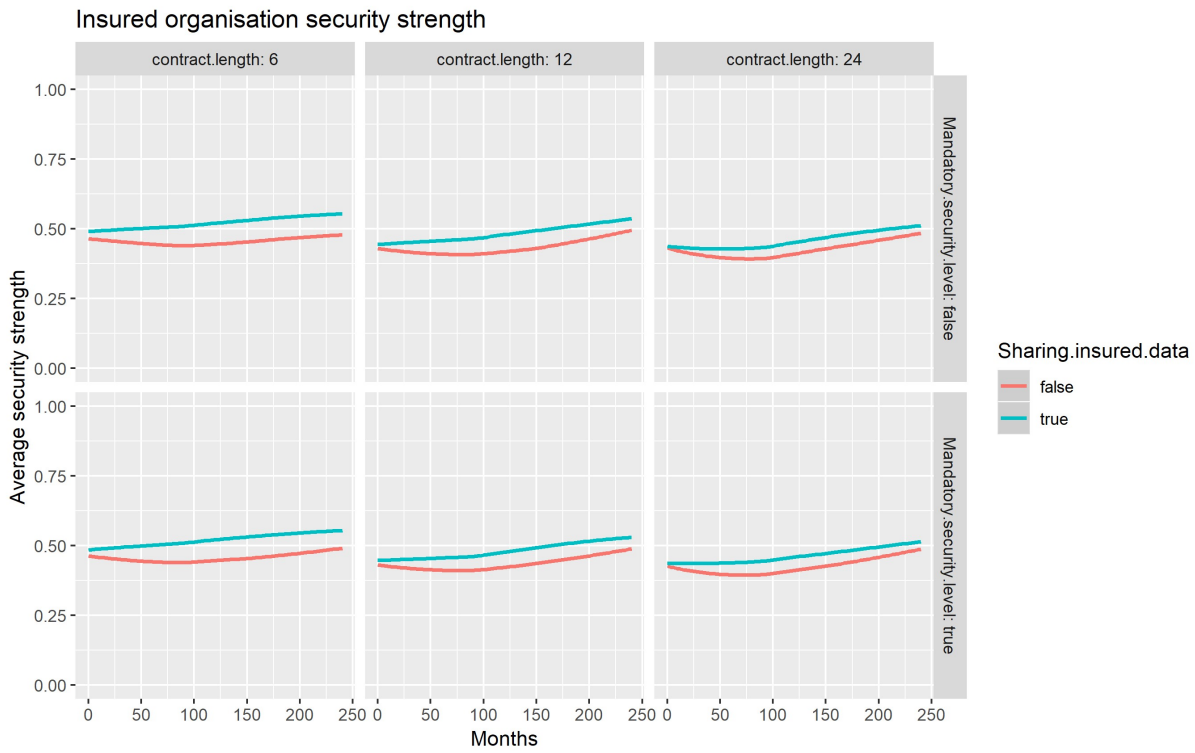

Figure 7-16: Facets on the influence of contract length, required security level and sharing control data on the cyber security level of insured organisations

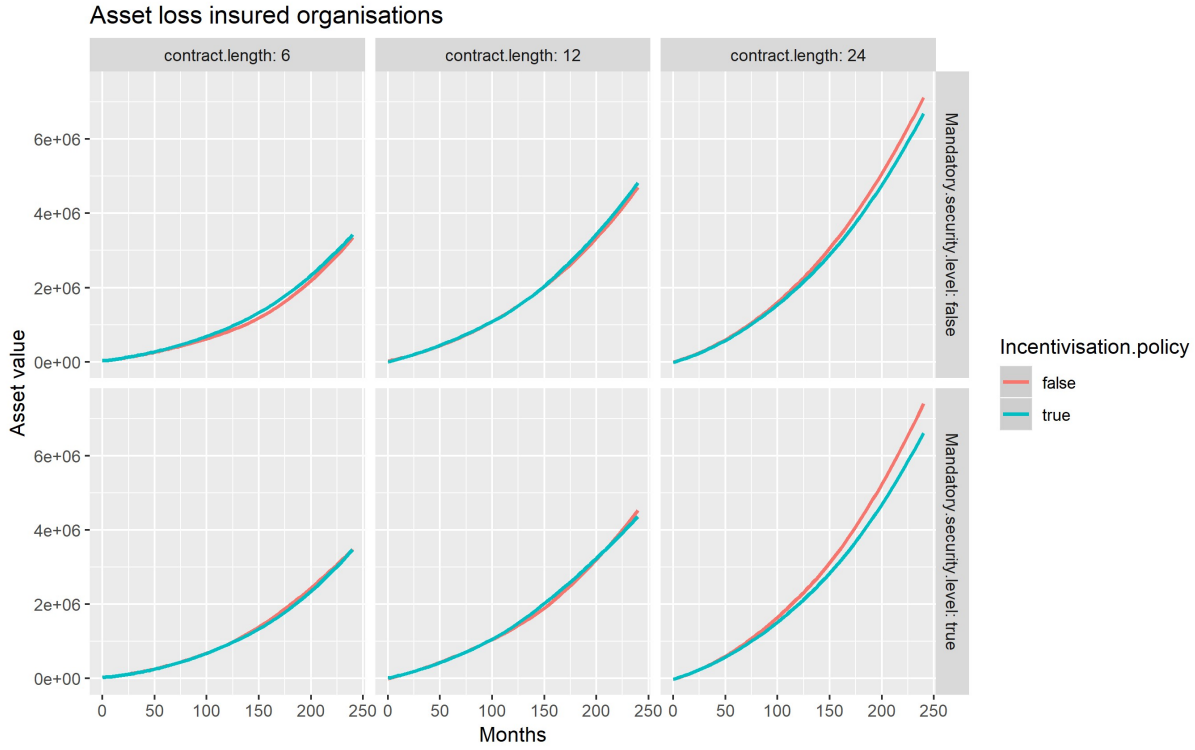

Figure 7-17: Facets on the influence of contract length, required security level and incentivisation on the value loss of insured organisations

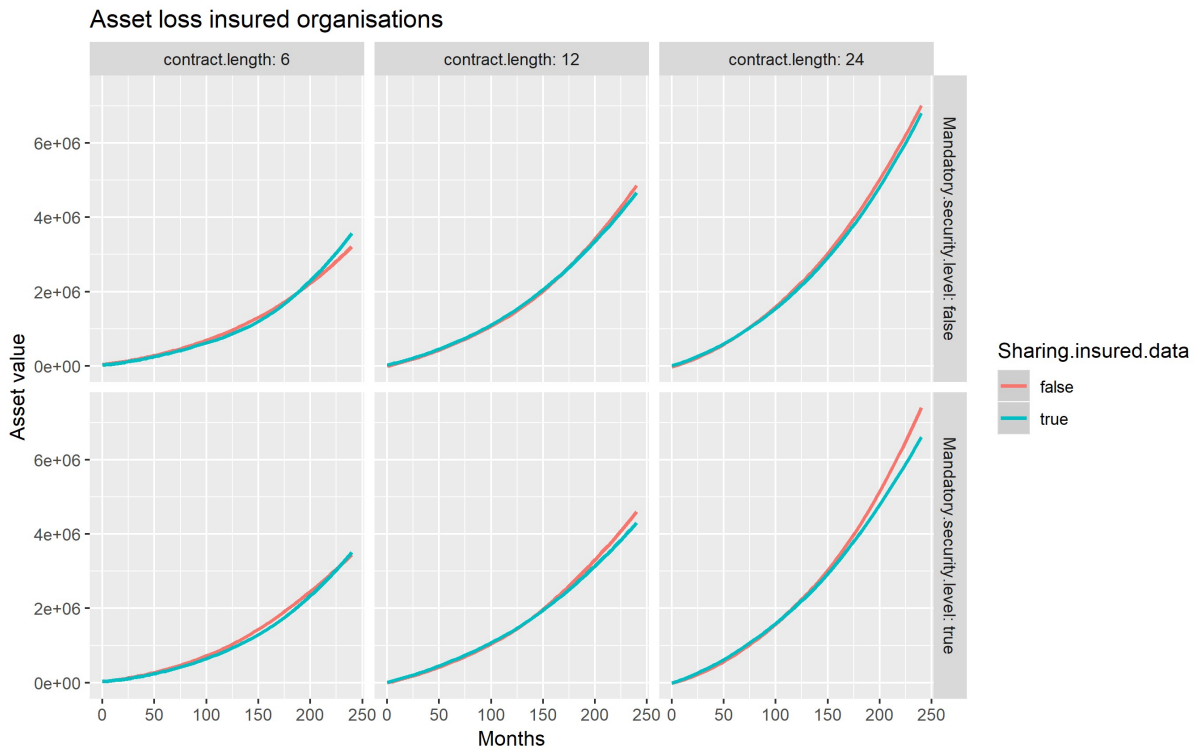

Figure 7-18: Facets on the influence of contract length, required security level and sharing control data on the value loss of insured organisations

7.2.3 Synergy experiment results

The setup for the synergy experiment was discussed in the section above. The setup will be run in the same way as the individual experiment analysis and will be measured using the same metrics. In figure 7-19 the influence of each synergy experiment and the baseline are shown on the cyber security strength of organisations. Synergy experiment 1 contains the contract length of 6 months, experiment 2 contains the contract length of 12 months and experiment 3 contains the contract length value of 24 months. The baseline is the same as it was for the individual experiment analysis. This means that each insurance option has been set to not influence the system, except for package options (option 1) and contract length (12 months). In order to gain more clarity into which of the contract length values has the best performance, it is useful to look at the global security strength. In the graph for the global security strength, it is clear that synergy experiment 1 performs the best. Furthermore, it performs much better than the baseline, which can also be seen in the graph of the cyber security strength of insured organisations. However, it also shows that fewer organisations are insured, as was expected of the contract length that is used in this experiment. That said, because the global security strength has become higher, it can still be concluded that it performs better than the other setups when it comes to security strength. However, looking at the global value loss, it seems that there is no observable difference between the setups. The values are very close but it seems that the synergy experiment 1 performs the best out of the four setups. In contrast, the performance in the asset loss of insured organisations is by far lower than the other setups for experiment 1. However, this could partly be attributed to having fewer insured organisations since the global value loss shows a rather small difference.

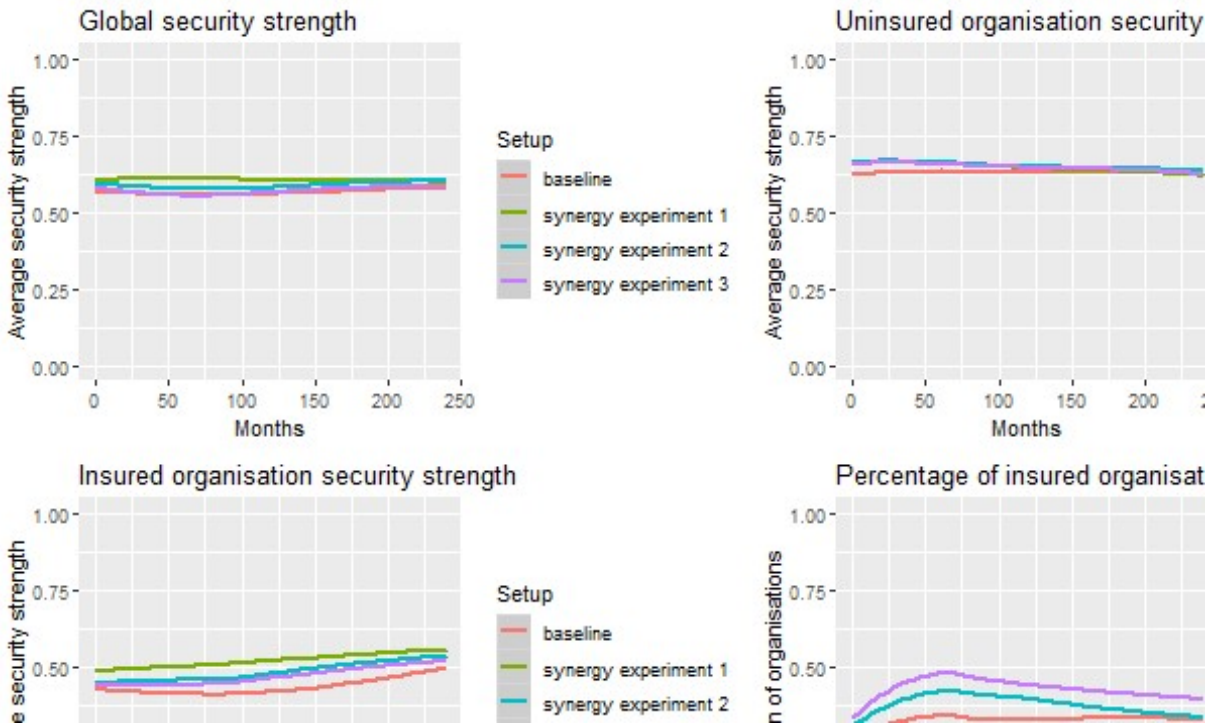

Figure 7-19: Influence of synergy experiments on the cyber security strength of organisations

Figure 7-20: Influence of synergy experiments on the asset loss of organisations

Figure 7-19 and 7-20 seem to indicate that synergy experiment 1 is indeed a useful setup with positive influences on the ecosystem. However, the influence that is brought forth by the setup might very well be based on the assumptions made in the model. For one, organisations do not act strategically to take advantage of the incentivisation policy. If they did, incentivisation could lead to a higher number of insured organisations and prevent them from dropping insurance. Another design

choice involves the information that is shared. The sharing of data causes a constant increase to the investment effectiveness, whilst in reality the effectiveness will depend on the circumstances. However, it is still possible that the observed effect will still occur in the actual system, the influence might even be stronger. Furthermore, the insurance options have a very clear intended effect making it possible to understand how they can bring forth positive effects (higher security and lower the losses). In most cases the options cannot lead to a negative scenario either, which makes it worth considering for implementation.

7.3 General analysis

Seven experiment parameters were used to influence the system. For each of these parameters, the goal was to observe if and how they influence the system. For each parameter, the results showed rather small influences on the global metrics. However, the graphs used for measuring the influence of the parameters on the only the insured organisations showed some more distinguishable differences though still seemingly small.

For the global metrics, the small differences can be explained by looking at the number of organisations that has bought insurance. Organisations are rational entities that make decisions based on what is in their best interest. This also holds true for the CRM process conducted by organisations in which they decide what to invest in. In this process they rationally go over each possible option they have to reduce risk with the intention to spend their budget efficiently. One of the options for organisations can be to buy insurance to mitigate risk. However, the premium asked by an insurance firm can be more expensive than the investment necessary to obtain an acceptable risk level. Furthermore, a design decision in the model is that organisations will prefer being uninsured if there was no possibility of reaching an acceptable risk level (none of the options could reduce risk enough or they were not viable). This leads to only a relatively small number of organisations to buy insurance, whilst the effect of the experiments can only be expressed through the insured organisations. Thus with lower amounts of insured organisations, less influence is visible in the global metrics. However, the main issue with insurance comes into play when larger amounts of insured organisations are present. The main issue is that insurance will always lead to lower cyber security strength because it costs money and can also allow organisations to reach an acceptable risk without investing in controls. Thus, when more organisations are insured these negative effects become more noticeable and undo some of the benefits obtained from insurance policies. This together with the performance for uninsured organisations then averages out and ends up providing little effects on the global metrics. Take mind that the negative influence of cyber insurance effects the value lost to attackers and does not have to reflect the welfare of the organisation as a result of being insured, this will be further discussed in the next chapter.

The small differences seen in the metrics for insured organisations can be explained through the downside of insurance. Insurance can be a useful tool to mitigate risk for organisations. However, in order to obtain insurance quite a large amount has to be spent, which means less money for investments into cyber security. Furthermore, if the coverage of an insurance package is high enough then there is a higher chance of a moral hazard to occur. This also explains why the metrics used to keep track of losses show so little difference. Only cyber security is capable of lowering the amount of asset loss. Another reason for the small differences lies in the choices made in the model. The effect of each experiment parameter had to be chosen and modelled accordingly. However, the values chosen for each parameter greatly influences how effective the parameter is and thus its

influence on the system. Whilst, the values were chosen as being logical and realistic, there is still a chance that the effectiveness of a parameter was underestimated. However, the analysis still provides valuable insight. This is because it showed that certain parameters have a positive and/or negative effect in some way. Thus if parameters were underestimated or overestimated, the implicated effects can be predicted. Lastly, the choices made for the baseline parameter values could be influencing the runs. For example, the maximum acceptable at risk value represents the amount of risk that an organisation finds acceptable. For lower values, less risk would be acceptable which would make them invest more which could also influence their decisions to obtain insurance. The budget of organisations or the asset values they are setup with can also have an influence on their behaviour and decisions. However, since the baseline was determined based on the sensitivity analysis and on literature, it is highly likely that the effects would only become more pronounced and would not lead to unexpected results.

Each figure has also shown that the effects of cyber insurance only become visible near the end of each run, representing 20 years. This might seem odd at first but has a very logical explanation. The development inside the model is quite slow. The CRM process that is used by organisations to defend themselves from attackers is only conducted twice a year. Therefore, the influence of cyber insurance can only be exerted twice a year. Moreover, since the effectiveness of each insurance option is relatively weak, the effect becomes even less obvious until a long time has gone by. This could be caused by model choices, since the investment interval was chosen to be 6 months. However, as was explained in chapter 5, an interval of 6 months actually seems realistic for this process. Therefore, the relatively small effects might also be observed in the real cyber security ecosystem.

8. Conclusion and discussion

In this chapter the main findings, implications, limitations and future research will be discussed. In the main finding the answers to each sub question and the research question will be given. This is followed by the implications that this research has for academic research. Afterwards, the limitations are presented in which the shortcomings of the agent-based model and research methods used for this research are described. The conclusion is completed by a discussion on future research.

8.1 Main findings

In this section the main findings will be presented for each sub question. Afterwards, the answer to the research question is provided. This is followed up with the main contributions.

8.1.1 Answers to research questions

Sub questions

1. *What behaviour and decision making mechanisms are part of each actor in the cyber security ecosystem and how do these actors interact with each other?*

For this sub question each actor was described along with their behaviour and decision making mechanisms in chapter 3. Additionally, the interactions of the actors in the cyber security ecosystem were determined. Below the behaviour and decision making mechanisms will be discussed for each actor, followed by their interactions in the cyber security ecosystem.

In the cyber security ecosystem, organisations are entities that are attacked for their asset value. This causes organisations to behave rationally and defend themselves whilst balancing the savings from successfully defending against the investments in cyber security (Cavusoglu et al., 2004). In order to defend themselves, organisations perform a process called Cyber Risk Management (CRM). In this process the organisations assess their risk, which can be defined as the probability of an attack occurring and the probable amount of value lost to it (Jones et al., 2005). Managing this risk is vital for an organisation and thus the ideal situation would be to have no risk at all. However, this is simply not achievable because attackers are continually adapting and new vulnerabilities are continually found. Therefore, an organisation also has a certain amount of risk that they find acceptable. Investing beyond the acceptable risk is deemed as unnecessary as it will result in reduced gains in the end (Salter et al., 1998).

There are various types of attackers that organisations have to deal with. These entities attack organisations for different reasons. Most attackers are after money but there are also attackers that target intellectual property, customer data or simply want to do damage to name a few (Rosenquist, 2009). Furthermore, attackers all have different capabilities which can make it more difficult to defend against. The reasoning and motivations of attackers has been standardised in some way into attacker profiles. This makes it possible for organisations to discern between the threat that each attacker forms. Attacker capabilities can involve many characteristic depending on the situation, but usually contains at least their motivations, time, budget and skills (Nostro et al., 2014). Attackers have a multitude of tools at their disposal. For instance, malware, viruses, phishing or more forceful attacks like DDoS / brute force or even make use of vulnerabilities. Each measure or tool has a different effectiveness as well. Phishing won't have the same success rate or gain as making use of vulnerabilities for example. However, depending on their resources not all tools can be obtained by an attacker. It is much harder to obtain and also more expensive to buy vulnerabilities compared to

obtaining malware. This makes every attacker diverse in their profile but also in the tools they utilise to attack organisations.

Insurance firms are essentially organisations that sell risk displacement as their product. Therefore, making a profit is also the goal of insurance firms. As such, the product they sell needs to be profitable which is done through insurance policies. These policies indicate what premium needs to be paid, how much is covered and can also contain additional conditions. In essence an insurance firm never rejects an organisations' request for insurance, instead the organisation receives a tailored insurance premium (Herath & Herath, 2011). This premium reflects the risk that an insurance firm will have to take on to insure the organisation and is used to ensure that the insurance firm earns more than it pays out. The coverage is also a tool to prevent taking on too much risk as it defines the maximum pay out that the insurance firm could ever make. Additional conditions are not of direct influence on the premium or coverage but can refer to conditions that must be met in order for insurance or insurance claims to be valid. For example, the insurer could require a certain amount to be invested into cyber security on a yearly basis. Not adhering to the insurance policy conditions therefore means that the contract is cancelled.

Insurance firms and organisations interact in two separate activities. The first interaction takes place during the CRM process conducted by organisations. In this process the organisations assess risk and determine their possibilities. They also consider cyber insurance as one of their possibilities, thus they contact the insurance firm to inquire what premium and coverage they would get. The insurance firm calculates a price depending on several factors, including the risk the organisation carries. If an organisation determines that obtaining insurance is the best way to go, they will formalise a contract with the insurance firm for the specified premium and coverage. The second interaction occurs when an insured organisation has been breached by an attacker. The organisation that has been breached will make an insurance claim to the insurance firm. The insurance firm will then assess the damages and losses and will pay out accordingly.

2. *Which insurance policies can be used by insurance firms and what factors make up these policies?*

This sub question was focussed on understanding the policies of insurance firms better. The aim was to identify the options insurance firms have to setup their policies. The information to answer this sub question was described in chapter 3.

The base elements used in an insurance policy are the premium and coverage. Additionally, the contract length is also specified in the insurance policy. However, there are also additional options for insurance possible. The following insurance options were identified and discussed:

- *Risk selection:* This option entails discriminating organisations based on their cyber security level. In this way, the insurance firm can prevent taking on risk without adequate financial compensation.
- *Incentivisation:* For this option, the insurance firm grants organisations, which invest adequately into cyber security, a reduction on their premium. By doing this the insurance firm can motivate organisations to keep investing in their cyber security reducing the chance of a moral hazard occurring.

- *Integration:* The insurance firms can also make use of integration. This means that the insurance firm will take on the CRM processes of an organisation. By doing this, increased investment efficiency can be achieved since the insurer gathers its knowledge its clients giving it better skill and understanding than an organisation by itself.
- *Upfront risk assessment:* For this option, organisations are required to pay for an upfront risk assessment when they buy insurance. The upfront risk assessment is used to reduce uncertainty for the insurance firm and also provides organisations with an assessment of their cyber security. This can be beneficial to both parties, the insurer has a better idea of the risk it takes on and the organisation has gained information on the vulnerabilities in its security.
- *Sharing cyber security control information:* Since the insurance firm has multiple clients, there is the possibility of sharing cyber security data. This data can help organisations with assessing their cyber security but also in deciding what controls to purchase.
- *Requiring organisations to maintain their security level:* This option entails making it mandatory for an organisation to maintain the security level they had when they bought insurance. This provides insurance firms with more certainty about the risk and also forces organisations to keep investing in their cyber security.

3. *In the modelled system of organisations and attackers, how does the system react to various policy setups employed by insurance firms?*

This sub question was answered in chapter 7. The main focus of this question was to identify how the previously identified insurance options influenced the cyber security strength and the value loss of organisations in the model. Seven options were used for experimentation, the analysis results were as following:

- *Insurance package options:* The insurance packages consisted of a base insurance premium and coverage. The experiment showed that the package options had a large effect on the number of insured organisations. Indicating that larger and more expensive packages lower the number of clients for the insurance firm. It also showed that for a smaller but cheaper package options, the cyber security of insured organisations is higher compared to the other package options. However at the same time the package options reduce the global security strength in the system. Concerning the value loss, the insurance package options had very little effect.
- *Contract length:* The contract length if of influence on the number of users as well. For longer contracts there are more cyber insurance users. However, the longer commitment also results in lower cyber security of insured organisations in initial stages, eventually performing similar to other contract lengths. The parameter had little to no effect on the global security strength. On the global value loss, the shorter contracts seem to lower the value slightly but other than that no real effects were found.
- *Risk selection:* Risk selection has one clear effect on the system: it reduces the number of organisations that are insured. It does increase the cyber security strength in the organisations that purchased insurance. Though this effect is attributed to giving better secured organisations a lower price. Similarly to the effect on cyber security strength, the

amount of value loss is lower for insured organisations. However, this is once again attributed to having very few but well secured organisation insured.

- *Incentivisation:* This option showed little difference compared to the baseline situation. It would seem that organisations would nearly always invest the amount necessary to qualify for a premium reduction just to keep risk low enough to be acceptable. However, the incentivisation policy did have a small positive effect on the amount of global value loss (less value lost).
- *Upfront risk assessment:* Upfront risk assessment had a positive influence on the cyber security strength of insured organisations. Furthermore, it also caused an increase in the number of insured organisations. However, since more organisations became insured, it also caused a very slight decrease in the global security strength. Concerning value loss, this option also caused a very small decrease in the global value lost.
- *Sharing cyber security control information:* Similar to the upfront risk assessment, sharing cyber security control information also had a positive effect on the cyber security strength of insured organisations. Furthermore, it had a slightly positive effect on the global security strength as well. The same can be said about the effect it had on the global value loss, there is a very small but positive effect.
- *Requiring organisations to maintain their security level:* Requiring organisations to maintain their cyber security level seemed to have no visible differences compared to the baseline situation with regard to the cyber security strength. However, it did have a very small positive effect on the global value loss of organisations.

4. *What insurance policies can be designed to lower damages across the ecosystem?*

The last sub question focusses on designing an insurance policy. This sub question was answered in chapter 7.

The insurance policy designed consisted of 4 parameters with the following values.

- Contract length: 6 - 24
- Required security level: true
- Incentivisation: true
- Sharing control data: true

The other values used were taken from the baseline experiment. The experiment showed that the design including a contract length of 6 (synergy experiment 1) was capable of influencing the system more than the individual options. The designed policy showed a higher global security strength value compared to the baseline and other design experiments. This effect was also observed in the cyber security strength of individual organisations. The global value loss showed a slight difference, showing that synergy experiment 1 slightly lowers the global loss. Whilst, graph for the value loss of insured organisations had a more clear distinction showing that there was less loss for insured organisations.

Research question

How do various cyber insurance policies affect the total damage in the cyber security ecosystem over time?

Several insurance policy setups have been described and experimented with. But before explaining the effects of the insurance policies, the general effect of cyber insurance should be acknowledged. The general effect that cyber insurance has on the system is that it lowers the cyber security strength of organisations. Therefore, the main effect it has on the total damage is that it will increase. This is because insurance in general is based on selling risk displacement, meaning the risk is given to a third party. However, displacing risk does not mean any steps were taken to preventing risks to occur in the first place. Furthermore, insurance costs money, thus processes relying on budget will suffer as a result. This is exactly the case for the cyber security ecosystem, the budget which is normally invested in cyber security controls are partly used to obtain insurance. Furthermore, organisations are rational entities, wanting to make the most of the money they spend. Therefore, if insurance covers the risk up till the amount they find acceptable, then they will invest less or even stop investing (moral hazard). Additionally, the lower security strength can also leads to more attacks and can cause more value being lost to attackers. However, insured organisations can actually be better off since they can claim losses from the insurance firm. Thus in the long run organisations can end up spending / losing less money compared to not being insured. The negative effects of cyber insurance can mostly be observed when the insurance policy used consists of a premium price, coverage and nothing else. By using additional conditions in the insurance policy, the insurer can control the situation more and might even be capable of circumventing the downside of insurance. This is why it is necessary to understand the influences of various insurance policies.

The experiments done to identify the influence of various insurance policy options have varying results. Individually, some of the policy options are not capable to change anything above the baseline. Most of the policy experiments resulted in very small differences between it and the baseline experiment as was discussed for sub question 3. However, there were some differences observable and most of them were positive. So whilst there were no large changes, all experiments showed positive effects also when it came to the total damage. However, some of the experiments had the downside of reducing the number of insured organisations. Based on the experiments done and their performance, a selection was made of policy options that might prove synergetic when put together and increase the effect, which was discussed above for sub question 4. This was indeed the case and resulted in more observable differences between the baseline and the experiment. The designed experiment was capable of reducing the damage loss for insured organisations. However, the total damage in the system only enjoyed a small decrease compared to the baseline.

The small influences of insurance policies can be attributed to the values used in the ABM model for the respective effects of each option. The values used for these effects had to be assumed since there is no actual data on how much effect it can have. However, whilst this may be the case, the model was still built on the premise that these values are logical and realistic. Therefore, there are possibilities that the effects can become more pronounced if the values for the effects are increased in the real system. An example of this is sharing control information, if the insurer can increase the effectiveness of this then the positive effect it has would grow with it. This would contribute to the security strength which is the one thing that affects the total damages done in the system. Additionally, by being able to make organisations stronger cyber security wise would increase the utility of cyber insurance thus leading to more insured organisations.

8.1.2 Main contributions

With the sub questions and research question answered. The main goal of this thesis has been fulfilled. In this section the main contributions of this research to the academic and societal fields will be discussed. The trigger for this research, the knowledge gap, as stated in chapter 1 consisted of clarifying the effects of cyber insurance and its insurance policies on the cyber security ecosystem. Furthermore, one of the large issues with academic literature was the lack of dynamicity in the research of the influence of cyber insurance.

Influence and synergy of various cyber insurance options

In literature there is hardly anything available on the possible options that insurance firm have to influence the ecosystem. Furthermore, there is even less available on the combined effects that these options can have. Theorising is simple, because the expected effects of the insurance policy options are quite logical. However, theorising and testing can give two very different results. Therefore, testing the various options and observing the impact they have on the ecosystem is required. That is how this research has contributed to academic knowledge. In this research these options have been further specified and implemented in an ABM model followed by experimentation in a dynamic environment, thus providing more insight on how much influence these options have or can have. Furthermore, this research has also designed and tested a synergy between several potential insurance policy options. This has provided insight on the combined effects that an insurance policies can have on the cyber security ecosystem.

Dynamic representation of the cyber security ecosystem

The final contribution is the creation of a dynamic agent-based model that simulates the cyber security ecosystem. A dynamic model capable of simulating the cyber security ecosystem in its entirety has not been created or used in academic literature yet. Therefore, the ABM model itself is also a contribution. Within the model it is possible to make changes to a multitude of parameters in order to influence the system. Providing the opportunity to experiment and analyse how the patterns and emergent behaviour can change. With more advanced knowledge or a background in ABM, it is also possible to adapt the model code in order to expand it or change the base variables it was built upon. This gives many possibilities for future research including the use of real values to simulate real world scenarios and experimenting with more detailed mechanisms and insurance policies.

8.2 Implications

8.2.1 Implications for academic research

In current academic literature there are quite some researches that have been done on the effects of cyber insurance. However, as was mentioned in the literature review, the research done tend to focus on a single entity and/or have used conceptual and mathematical model. Furthermore, there is very little literature available on the synergies between insurance policies. The research done in this thesis has simulated the cyber security ecosystem and can give answers from a dynamic perspective. This is something that was missing from most literature on the effects of cyber insurance. Furthermore, the agent-based model provides an ecosystem view of the influence of cyber insurance. This makes it possible to gain much more insight about the effects and can give more detailed answers to many of the questions asked in literature. For instance, Bandyopadhyay,

Mookerjee, & Rao (2009) researched why growth for insurance firms in the market is difficult. One of the statements made in the paper, is that premiums tend to become overpriced. Using the ABM model of the cyber security ecosystem it becomes possible to see when the insurance premium becomes too expensive. Furthermore, the additional effect surrounding pricing can be added in order to provide even more accurate data on pricing strategies. This would also make it possible to test the various solutions proposed by the paper. Additionally, the effect on the losses of organisations can be measured as well. In literature there is also a lot of research done with conceptual and mathematical models (Pal & Golubchik, 2010; Pal et al., 2014; Yang & Lui, 2014). However, as the ABM model showed, there is quite some chaos in the cyber security ecosystem. Using mathematical model is useful but usually only in specific situations focussing on one entity at the time. By using the model these conceptual and mathematical models can be run with multiple agents in a simulation that represents the real ecosystem. This can provide more insight into whether the effects theorized would still be able to manifest when all actors are present and how effective it would be. Furthermore, because the model can be used to measure all kinds of output of the agents, the direct and indirect effects can be analysed. For instance, Gordon et al. (2003) writes about how cyber insurance can be beneficial to the reduction of cyber risk. However, they did not write about the indirect effects it has on the cyber security level or the asset losses of the organisations that buy insurance. This research has shown that insurance firms have indirect effects on the cyber security strength and it has shown how large this effect is. As such, seeing the benefits of a dynamic approach, it is expected that more dynamic models will be created or used to answer various questions about cyber insurance.

8.2.2 Detailed insurance policy design and testing

There is very little literature available on the possible cyber insurance policies that can be used by insurance firms to affect the system. Many have researched if cyber insurance can be useful to cyber risk management or whether its displacement of risk can measure up to the costs of obtaining insurance. However, very little has been written about how an insurance firm can become a positive effect on the organisations in the ecosystem. Part of the reason for this is because there is a lot of uncertainty surrounding the actual effects of cyber insurance, a lack of visualisation and data. The ABM model created in this thesis can take away some of these concerns and provide the means to start exploring the possible interventions that an insurance firm, or policy maker for that matter, can implement in order to bring a positive effect to both insurance firms and organisations in the ecosystem. Furthermore, by adjusting the mechanisms and changing base variables, it is possible to adapt the model to specific situations. However, the model built in this thesis should just be the beginning. Using modelling tools, cyber insurance can be better explored. Thus it would be expected that modelling tools will be utilised more for exploring the cyber security and cyber insurance landscape.

8.3 Limitations

In this research the effect of cyber insurance policies on the cyber security ecosystem has been performed using an ABM model. The model was conceptualised and built based on literature and it also forms the foundation for all the results that have been generated. However, there are several factors that can prove to be limitations which can influence the validity, representativeness and insights. By acknowledging and discussing these limitations, any doubts in the research can be clarified.

Ecosystem level abstraction

One of the limitations of the model is that the ecosystem has had to be abstracted before it could be modelled. This is because not every single detail can be simulated since it would make the simulation too heavy on resources to run. Furthermore, adding more details to a model can take a lot of time, thus it was also not feasible to add more details to the model within the timeframe of this thesis. For abstraction the less important parameters and variables are reduced, leaving the important and most interesting behaviour intact. Abstraction can have consequences for the model behaviour since it usually involves reducing complex mechanisms to simpler ones, substituting in a static value or even removing them entirely. Additionally, abstraction is based on the modellers' perspective of the system. Thus it means that certain details can be missed and that if someone would model it, the system might work in a different way. However, the modelling steps used in this thesis help in creating a stable basis and to ensure the right mechanisms are modelled. This is also why the verification step is necessary and very useful to modelling studies.

Lack of realistic data as input

Another important limitation is the lack of realistic data to use as input. The cyber security ecosystem is very difficult to model since it is very hard to draw scope the system by stating the number of organisations and attackers. Furthermore, once a scope is determined, there is still the issue of determining the values that agents should be given. The data available is mostly on aggregated level and thus could not be used for the model. Therefore, the model has had to be built by validating the mechanisms and balancing the parameters in order to achieve realistic behaviour and patterns. Because of this the results cannot be translated to reality. However, the perceived behaviour and effects would still be the same as they would be in reality. As such, the model has an exploratory function, meaning that it is more useful to exploring the effects of various interventions.

Assumptions on agent mechanisms

As mentioned in chapter 4, several assumptions have been made in order to gain an abstract the system and thus to create the agent-based model. These assumptions do not have to be problematic but they do limit the model in a sense. The assumptions simplify model behaviour and can therefore remove important aspects of agents. Furthermore, the assumptions made, can lack the detail that could be used to make the agents in the model more dynamic and autonomous. However, these simplifications were made because it was expected that the specific mechanism wouldn't have much effect on the results.

There were three important assumptions made. The first is using only one value for the assets. The second is that organisations are not strategic in the sense of planning ahead. The third is that organisations only enter a state of recovery after being breached.

The first simplification has great consequences for the behaviour in the model. However, implementing multiple asset values can greatly increase complexity and also make the model too heavy to run / experiment with. The behaviour that would be added by adding multiple asset values would give the model much greater dynamicity. This is because it would allow attackers to choose a more specific target. Furthermore, it could introduce additional elements that could be part of the CRM process. For instance, intellectual property could be valued more, thus changing the acceptable risk or making insurance unfavourable. It could also lead to more extensive insurance packages that target specific assets. However, it should be kept in mind that this would mean that a large part of

the code would have to be redesigned to accommodate this change. This combined with the complexity increase might not be worth it. If organisations would have different types of asset value, the current experiment might show different results. It is likely that fewer organisations would choose to be insured since insurance does not prevent being breached it only pays out the damages financially. Thus organisations that do not want their assets stolen in the first place would rather invest in their own security as much as possible. Furthermore, attackers would select their targets based on the type of asset value it would want to obtain. This would affect the risk that an organisation faces and thus the outcome of their risk assessment. The insurance firm would in this case also become able to use different coverage limits for each type of asset. This could lead to package combinations that can appeal to specific organisations.

The second simplification concerns not planning ahead. This assumption was made because it is simply very difficult to make an organisation predict and remember in order to make long term strategic decisions. However, since it did impact the experiments, it is worth mentioning because it is possible that other (new) insurance policies might suffer from the same design choice. Strategic behaviour could increase insight a lot, since organisations are very rational entities. Strategic thinking is something these entities are involved with on a regular basis. Furthermore, when looking at the results in this thesis, strategic thinking could lead to different results. First, it would make organisations exploit the opportunities that the insurance firm can provide. This can lead to more organisations becoming insured. Second, strategic behaviour can also include an organisation to keep track of its 'loss history'. This could lead to organisations adjusting the inaccuracy of their assessment in order to obtain a more accurate risk on which to base new decisions. Third, organisations would forecast the costs they expect to make with and without insurance in an attempt to minimise costs. This would especially lead to different results with longer contracts, since it would mean having to pay premiums until the end of it.

The third simplification has to do with only going into a state of recovery and nothing else. This can be a troublesome assumption, since in reality, when an organisation is attacked they will reallocate budget in order to respond to the threat. During this time, they would patch vulnerabilities and might even upgrade their security controls. This could provide the model with much more interaction and would let organisation behave more natural. Furthermore, it could impact the results of the model since organisations would be able to spend more than just their annual budget. As a result, by incorporating a response procedure, much more accurate and useful information could be obtained whilst exploring the system.

8.4 Future research

In this section the possible future research will be discussed. Several suggestions for future research have been formulated based on the results of this thesis.

The first suggestion is to continue using the ABM model that was created in this thesis to experiment with and design new insurance policies. The model is a powerful tool that can help in determining the effects of various policy setups. Furthermore, the model can be expanded upon by adding more parameters which will allow for the design of new policies and testing their effects. New insights can be gained by exploring the model behaviour which could possibly lead to insurance policy designs that are much more effective at influencing the ecosystem.

The second suggestion is to further specify and detail the mechanisms used in the ABM model. The model in its current state is still quite abstract. By further specifying mechanisms in the model, the behaviour can be made more realistic. For example one of the artefacts of the model was the lack of strategic behaviour of organisations when it comes to incentivisation. By adding a strategic mechanism, the model behaviour could start giving new insights into the effects of incentivisation or the combination of it with other mechanisms.

The third suggestion is to start using dynamic models more for the cyber security ecosystem and for cyber insurance. The threat landscape is dynamic in nature, being unpredictable and chaotic. This greatly influences organisations as a result because they base their CRM process on the threat landscape. Using conceptual and mathematical model can provide some insight. However, because of the dynamic nature of the ecosystem, its actual effects could still be different than was originally expected simply because of the interactions within the system.

References

Augusiak, J., den Brink, P. J., & Grimm, V. (2014). Merging validation and evaluation of ecological models to 'evaludation': a review of terminology and a practical approach. *Ecological Modelling*, *280*, 117–128.

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), 68–73.

Betterly. (2015). *Cyber/privacy insurance market survey 2015: For Larger Insured, A Market in Turmoil, For the SME Insured, Eager Insurers Await*. Retrieved from http://betterley.com/samples/cpims15_nt.pdf

Bialas, A. (2015). Experimentation tool for critical infrastructures risk management. In *Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on* (pp. 1099–1106).

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), 131–158.

Blakely, B. A. (2012). *Cyberprints: Identifying cyber attackers by feature analysis*. Iowa State University.

Böhme, R. (2010). Security metrics and security investment models. In *International Workshop on Security* (pp. 10–24).

Böhme, R., Schwartz, G., & others. (2010). Modeling Cyber-Insurance: Towards a Unifying Framework. In *WEIS*.

Bolot, J., & Lelarge, M. (2009). Cyber insurance as an incentive for Internet security. In *Managing information risk and the economics of security* (pp. 269–290). Springer.

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

Chan, S. (2001). Complex adaptive systems. In *ESD. 83 research seminar in engineering systems* (Vol. 31, p. 1).

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27.

DeAngelo, H., & Roll, R. (2015). How stable are corporate capital structures? *The Journal of Finance*, *70*(1), 373–418.

den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boeke, S., van de Koppen, L., … De Bos, T. (2014). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. In *Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium* (pp. 13–14).

Denning, D. E. (2000). Cyberterrorism.

Desmos. (2018). Desmos graphing. Retrieved September 17, 2018, from https://www.desmos.com/calculator/

Dowling, G. R. (1993). Developing your company image into a corporate asset. *Long Range Planning*, *26*(2), 101–109. https://doi.org/https://doi.org/10.1016/0024-6301(93)90141-2

Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., … others. (2011). Symantec internet

security threat report trends for 2010. *Volume XVI*.

Gartner. (2016). Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016. Retrieved from https://www.gartner.com/newsroom/id/3404817

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81–85.

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

Herath, H., & Herath, T. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, *2*(1), 7–20.

Hoang, D. T., Wang, P., Niyato, D., & Hossain, E. (2017). Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: A cyber insurance-based model. *IEEE Access*, *5*, 732–754.

Holland, J. H. (1992). Complex adaptive systems. *Daedalus*, 17–30.

Innerhofer-Oberperfler, F., & Breu, R. (2010). Potential rating indicators for cyberinsurance: An exploratory qualitative study. In *Economics of Information Security and Privacy* (pp. 249–278). Springer.

Jerman-Blažič, B., & others. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413–422.

Johnson, B., Böhme, R., & Grossklags, J. (2011). Security games with market insurance. In *International Conference on Decision and Game Theory for Security* (pp. 117–130).

Jones, J., CISSP, CISM, & CISA. (2005). *An Introduction to Factor Analysis of Information Risk (FAIR)*.

Labunets, K., Pieters, W., & van Eeten, M. (2018). *CYBECO WP7: Cyber insurance ecosystem*.

Lansing, J. S. (2003). Complex adaptive systems. *Annual Review of Anthropology*, *32*(1), 183–204.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic & International Studies Washington, DC.

Libicki, M. C., Ablon, L., & Webb, T. (2015). *The defender's dilemma: Charting a course toward cybersecurity*. Rand Corporation.

Macal, C. M., & North, M. J. (2005). Tutorial on agent-based modeling and simulation. In *Simulation conference, 2005 proceedings of the winter* (p. 14--pp).

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M., & Sibley, C. (2015). The human factor in cybersecurity: Robust & intelligent defense. In *Cyber Warfare* (pp. 173–206). Springer.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61.

Moitra, S. D., & Konda, S. L. (2000). *The survivability of network systems: An empirical analysis*.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11–26.

Nostro, N., Ceccarelli, A., Bondavalli, A., & Brancati, F. (2014). Insider threat assessment: A model-

based methodology. *ACM SIGOPS Operating Systems Review*, *48*(2), 3–12.

Novak, P., Kadera, P., & Wimmer, M. (2017). Agent-Based Modeling and Simulation of Hybrid Cyber-Physical Systems. In *Cybernetics (CYBCONF), 2017 3rd IEEE International Conference on* (pp. 1–8).

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Digital Investigation*, *2*(4), 261–267.

Ögüt, H., Raghunathan, S., & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, *31*(3), 497–512.

Pal, R., & Golubchik, L. (2010). Analyzing self-defense investments in internet security under cyber-insurance coverage. In *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on* (pp. 339–347).

Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber-insurance improve network security? A market analysis. In *INFOCOM, 2014 Proceedings IEEE* (pp. 235–243).

Passeri, P. (2018). February 2018 Cyber Attacks Statistics. Retrieved April 17, 2018, from https://www.hackmageddon.com/2018/04/06/february-2018-cyber-attacks-statistics/

R Core, T. (2018). R: A Language and Environment for Statistical Computing. Vienna, Austria: R Foundation for Statistical Computing. Retrieved from http://www.r-project.org/

Ralston, P. A. S., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, *46*(4), 583–594.

Rosenquist, M. (2009). Prioritizing information security risks with threat agent risk assessment. *Intel Corporation White Paper*.

Rowe, B. R., & Gallaher, M. P. (2006). Private sector cyber security investment strategies: An empirical analysis. In *The fifth workshop on the economics of information security (WEIS06)*.

Salter, C., Saydjari, O. S., Schneier, B., & Wallner, J. (1998). Toward a secure system engineering methodolgy. In *Proceedings of the 1998 workshop on New security paradigms* (pp. 2–10).

Shetty, N., Schwartz, G., Felegyhazi, M., & Walrand, J. (2010). Competitive cyber-insurance and internet security. *Economics of Information Security and Privacy*, 229–247.

Tisue, S., & Wilensky, U. (2004). NetLogo: Design and implementation of a multi-agent modeling environment. In *Proceedings of agent* (Vol. 2004, pp. 7–9).

ulisi Ogut, H., & Raghunathan, S. (2005). Cyber Insurance and IT Security Investment: Impact of Interdependent Risk. *The University of Texas at Dallas*.

Van Dam, K. H., Nikolic, I., & Lukszo, Z. (2013). *Agent-based modelling of socio-technical systems* (Vol. 9). Springer Science & Business Media.

Verizon. (2018). *Executive summary 2018 Data Breach Investigations Report*. Retrieved from https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

Vraalsen, F., Mahler, T., Lund, M. S., Hogganvik, I., den Braber, F., & Stølen, K. (2007). Assessing enterprise risk level: The CORAS approach. *Advances in Enterprise Information Technology Security*, 311–333.

Wickham, H., & Chang, W. (2008). ggplot2: An implementation of the Grammar of Graphics. R package version 0.7. Retrieved from http://cran.r-project.org/package=ggplot2.

Woods, D. W., & Simpson, A. C. (2018). Monte Carlo methods to investigate how aggregated cyber insurance claims data impacts security investments.

Yang, Z., & Lui, J. C. S. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks ☆. *Performance Evaluation*, *74*, 1–17. https://doi.org/10.1016/j.peva.2013.10.003

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems*, *30*(1), 123–152.

Appendix A. Model verification

Van Dam et al. (2013) prescribe four main parts to model verification.

1. Recording and tracking agent behaviour
2. Single-agent testing
3. Interaction testing limited to minimal model
4. Multi-agent testing

Recoding and tracking agent behaviour

For this step the model behaviour is checked throughout a run. By doing this each agent can be checked to see if it is actually performing each procedure and ending up with the correct values.

This step was performed within the model itself and has been verified.

Single-agent testing

For single-agent testing the model is run with only one agent. By doing this, behaviour can be identified and verified for a single agent at a time. This step is set up in two parts. The first part is theoretical predictions and sanity checks. For this part, a theoretical description is given of the behaviour an agent will show after which a check is done to see if this happens. The second part is breaking the agent. For this part the agent will receive parameter values as to 'break' it. This will verify if the agent still acts logically when it receives extreme inputs. If it breaks, then the model will be adjusted to prevent it from happening again.

Theoretical predictions and sanity checks

Insurance firm: the insurance firm in the model does not do anything outside the setup. Therefore, no further testing is required.

Organisations

- The organisation will conduct the CRM-process and assess its risk level
  Confirmed

- The organisation will set its budget as its annual budget
  Confirmed

- The organisation will update its cyber security strength based on the cyber control effectiveness reduction
  Confirmed

- The organisation will update its assets value
  Confirmed

Attackers:

- The attacker will assess if there are any viable targets
  Confirmed

Environment

- Cyber risk controls will degrade
  Confirmed

Breaking the agent

Organisations

- The budget for organisations was set to -1000
  The agent showed a reduction of cyber security because a negative budget was invested. The value was overwritten by the annual budget at ticks mod 12 = 0. Negative budgets can potentially be breaking. However since this value should never appear in the first place, it does not have to be fixed.

- The cyber security strength of the organisation was set to -100
  The agent cyber security strength became -100. The organisation started investing in cyber security making the value move back up towards 0. This poses no problem, agent behaviour was unaffected.

- The asset value of the organisation was set to -100
  The organisations started mutating the asset value negatively, showing a negative growth. This is not necessarily breaking but the code will be adjusted to prevent this negative growth from happening.

- The assessment uncertainty was set to -50
  The organisation stopped investing because the risk was always below the acceptable risk. This was expected and therefore no problem.

- The assessment uncertainty was set to 100
  The organisation started investing maximally because the risk was always above the acceptable risk. This was expected and therefore no problem.

- The maximum acceptable risk was set to -10
  The organisation started investing maximally because the risk was always above the acceptable risk. This was expected and therefore no problem.

- The maximum acceptable risk was set to 10
  The organisation stopped investing because the risk was always below the acceptable risk. This was expected and therefore no problem.

Attackers:

- The skill level of an attacker was set to -1
  The attacker ends up not attacking at all. This was completely expected and thus no problem.

- The resource level of an attacker was set to -1
  The attacker eventually manages to get attacks in, the resource value is unchanged. This is caused by always defaulting to tool 1 for attackers, thus it can always proceed with an attempt to attack.

Interaction testing limited to minimal model

For interaction testing in a limited to minimal model, the lowest number of agents is added to allow for interaction to occur. For this model that means that one agent for each group is added: 1 organisation, 1 insurance firm and 1 attacker. The theoretical predictions and sanity checks will also be performed for this setup.

Insurance firm: the insurance firm in the model does not do anything outside the setup. Therefore, no further testing is required.

Organisations

- The organisation will invest in cyber security and increase its cyber security strength
  Confirmed

- The organisation will go through the CRM process and obtain a contract for cyber insurance
  Confirmed

- An organisation cannot have a budget lower than 0
  Error, value goes below 0
  Fixed, budget did not account for insurance payments and thus became negative

- With the cyber security level of the organisation set to 5 it will not be attacked by the attacker
  Confirmed

- With the cyber security level of the organisation set to 1 it will be attacked by the attacker
  Confirmed

- The cyber security strength of an organisation can never go below 0 or above 1
  Error, value goes below 0
  Fixed, budget became negative

- After being attacked the organisation will set its recovery timer to a random value between 1 and 6 and sets can-be-attacked? to false
  Confirmed

- The organisation will reduce its recovery timer every tick, once it reaches 0 it will set can-be-attacked? to true
  Confirmed

- With the acceptable risk set to 0, the organisation will always invest its budget when it can
  Confirmed

- Once contracted, the organisation cannot break the contract until the duration is over
  Confirmed

- Once contracted, an organisation cannot buy an insurance package that is lower than the package it is using currently
  Confirmed

- If upfront risk assessment is true, then the organisation will pay upfront risk assessment costs when buying insurance
  Confirmed

- If upfront risk assessment or sharing insured data is true and the organisation is contracted. Then its investments will be more effective
  Confirmed

- If the organisation cannot reduce risk to acceptable levels, invest 50% of the budget if ticks mod 12 = 0 otherwise invest 100%
  Confirmed

- If contract length > 11 and ticks mod 12 = 0, the organisation will reserve budget as to ensure that it can pay insurance in 6 months
  Confirmed

- If risk is acceptable, annual budget is reduced by 5%
  Confirmed

- If risk is not acceptable and all options are unable to reduce risk to acceptable levels, set annual budget + 5%
  Confirmed

- With insurance package 2 having an insurance price of 1 and other package of 100000, organisation should buy package 2
  Confirmed

- With budget and annual budget set to 0, the organisation cannot make any investments and does not conduct CRM process
  Confirmed

- If attacked and insured, claim damages from insurance firm and add to asset value
  Confirmed

Attackers:

- The attacker will set the organisation as viable and attack it if its skill is higher than the cyber security strength of the organisation
  Confirmed

- The attacker obtains a tool based on random values
  Confirmed

- After obtaining a tool, the attacker makes a success calculation. The agent attacks if successful or fails if unsuccessful
  Confirmed

- If the attacker is successful in its attack, it will calculate the amount of value it steals based on its skill and tool
  Confirmed

Multi-agent testing

The last step of verification is multi-agent testing. For this step all agents will be included and tested. In this step variability and timeline sanity tests will be conducted. For variability model runs will be repeated many times in order to assess the chaos in the system and to see if the all behaviour can be explained. Timeline sanity tests will show how the model performs at a representative setup and to see if there are any unexplainable readings.

Variability testing

Variability was tested during the sensitivity analysis in chapter 6. Therefore, it will not be discussed here.

Timeline sanity

For timeline sanity the following setup is used. This is the same setup as the baseline defined in chapter 6

- Organisation-budget: 8000
- Assessment-uncertainty: 0.2
- Maximum-acceptable-risk-percentage: 0.1
- Minimum-asset-value: 20000
- #Large-organisations: 40
- #Medium-organisations: 50
- #Small-organisations: 35
- #thiefs: 50
- #spies: 35
- #professional-hackers: 25
- #activists: 20
- Contract-length: 6
- Pay-out-factor: 0.95
- Insurance-package-1-coverage: 7500
- Insurance-package-1-baseprice: 4000
- Insurance-package-2-coverage: 12000
- Insurance-package-2-baseprice: 6250
- Insurance-package-3-coverage: 14000
- Insurance-package-3-baseprice: 8000

Based on these values graphs have been generated for the global security strength, global value loss, global asset value, total annual budget and number of insured organisations.

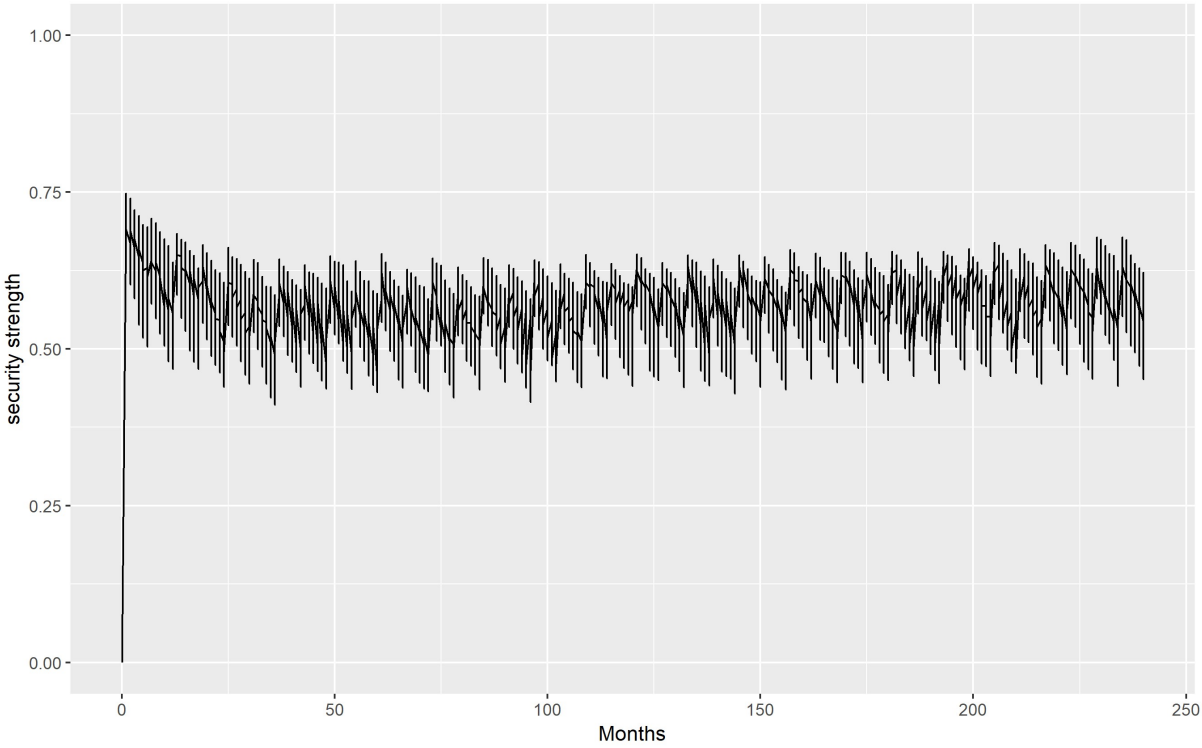

Figure A-1: Global security strength timeline sanity

Figure A-1 shows the global security strength. This run shows results that are expected. The security strength is being increased and decreased constantly throughout the run. This is caused by investment and reduction of cyber security effectiveness.

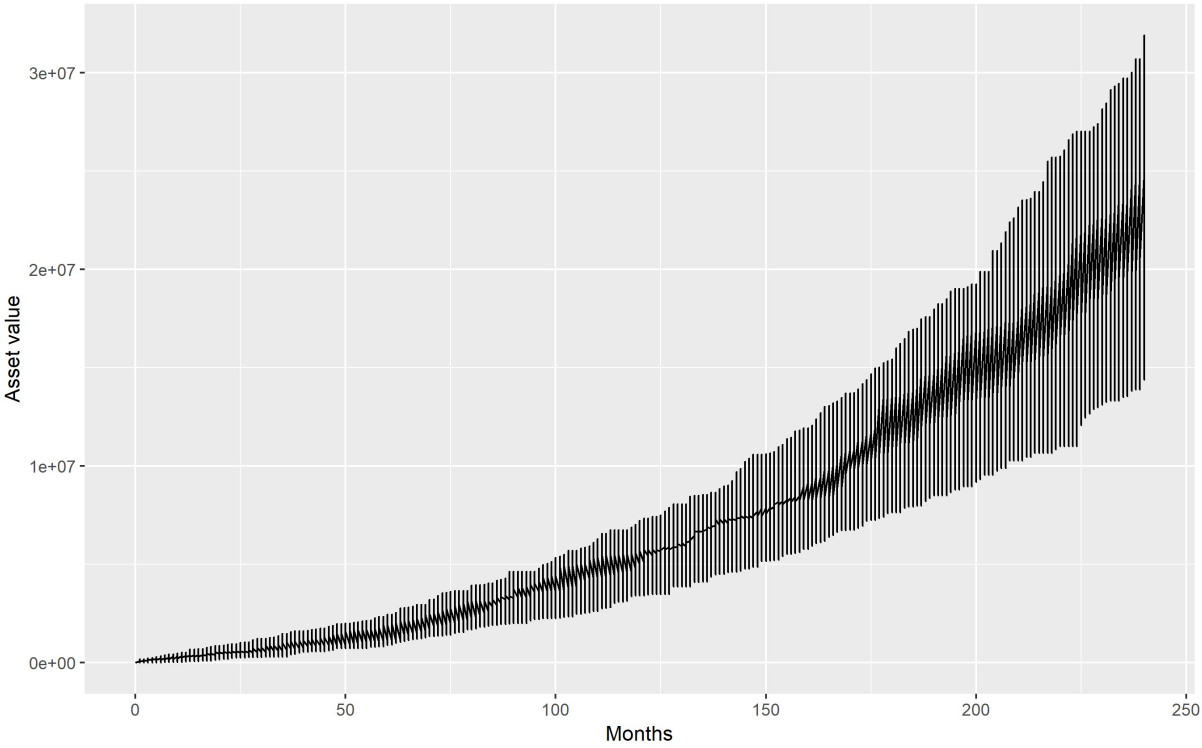

Figure A-2: Global value loss timeline sanity

The global value loss shows an expected pattern. There is some deviation, but this is to be expected since the initialisation gives organisations different amounts of values and attackers also affect these

values. The curve is also accumulative, thus it is logical that it ends up much higher than it started.

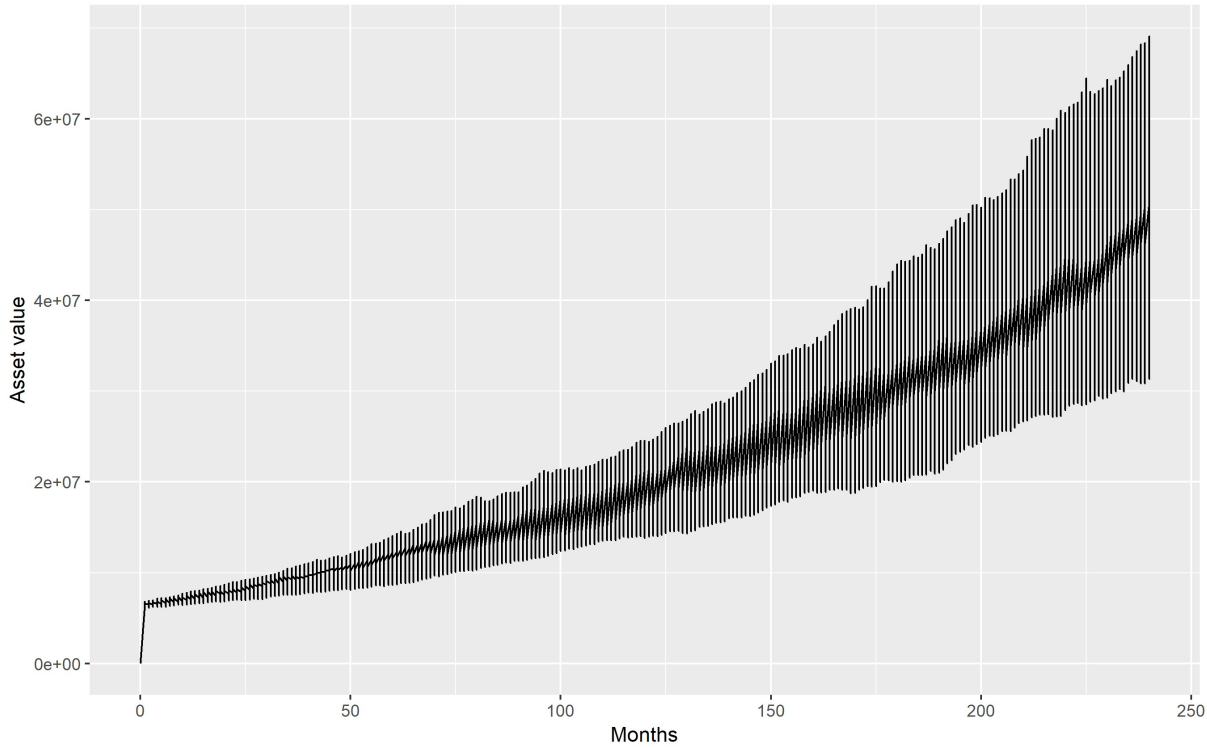

Figure A-3: Global asset value timeline sanity

The asset value curve is exactly as expected. Over time there is a gradual increase. However, the curve itself should show some peaks and troughs, which it does.

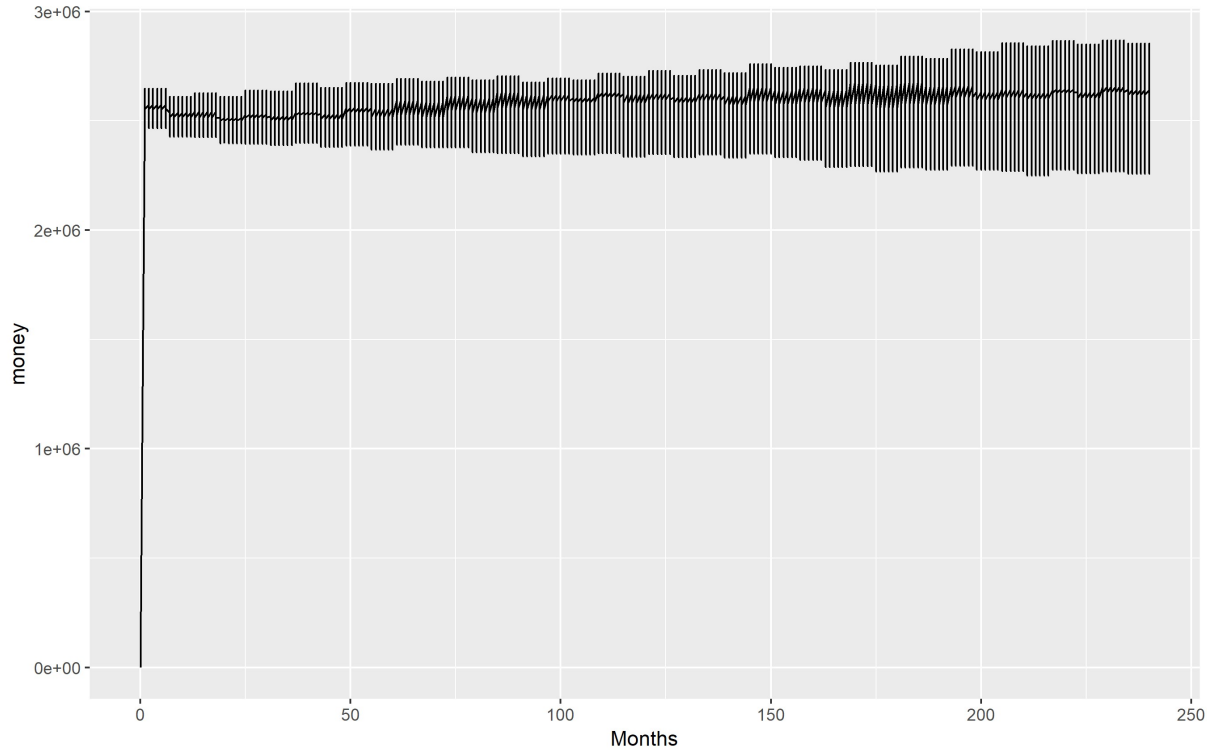

Figure A-4: Total annual budget timeline sanity

The total annual budget remains quite stable. This was to be expected since every run was the same. The slight spread can also be explained simply by the security strength organisations manage to

achieve. Depending on their security strength they can deem the risk acceptable and thus lower their budget.

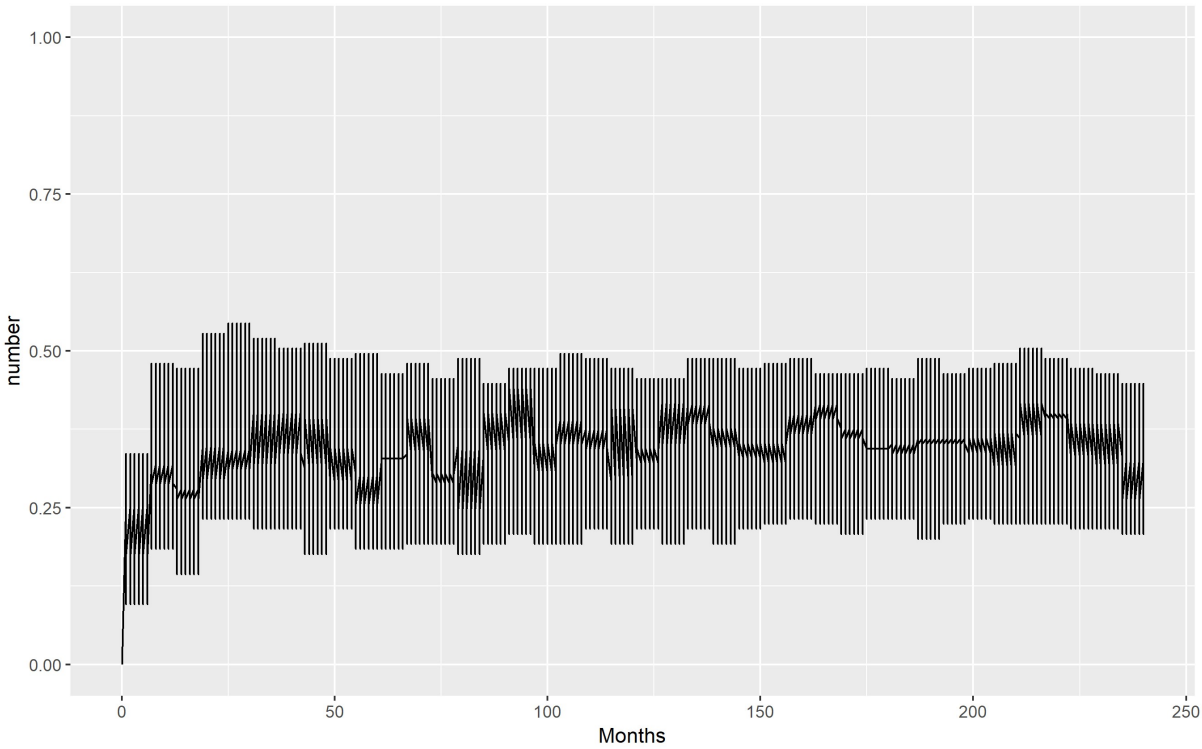

Figure A-5: Number of insured organisations timeline sanity

The graphs showing the number of insured organisations is also as expected. Since every run has some random values at initialisation, it is logical that there is some spread. However, every run seems to follow the same pattern.

Appendix B. Sensitivity analysis

Below the analysis of the data for the sensitivity analysis will be discussed for each parameter that was varied. The sensitivity will be analysed using the metrics for cyber security strength, annual budget and global value loss. These metrics were selected as they will provide the most information about the sensitivity of parameters and still keep the analysis possible with the limited computational power available.

Cyber security strength

As was explained in chapter 4, there are three cyber security strength metrics that are used in the model: cyber security strength globally, for insured organisations and for uninsured organisations. For the sensitivity analysis all three of these metrics can provide useful insight because the parameters can have an effect on their ability / desire to obtain cyber insurance. Thus only by analysing the data for all three metrics can insight be obtained concerning cyber security strength.

Global cyber security strength

The global cyber security strength for all four parameters is shown in figures B-1 – B-4. As can be seen in the figures, the cyber security strength tends to follow the same pattern for every parameter. This is logical since no matter the parameter value, each organisation will attempt to mitigate their risk until they find it acceptable or keep investing as long as it is not. As a result, the organisations end up around the same cyber security strength in every run. However, there are still differences visible between the values used for the runs.

Figure B-1 shows the effect of the budget of organisations on the cyber security strength. In this figure it is very clear that for lower a budget, the cyber security strength ends up lower and vice versa for a high budget. This is a realistic thing to happen, since a lower budget means that there is less money to invest in controls and it might even prevent organisations from being able to afford cyber insurance. Furthermore, it seems that for higher budgets, the spread patterns are overlapping quite a bit. This means that having more budgets does not increase the cyber security strength in equal steps. This is likely caused by organisations reaching an acceptable risk and thus refraining from investing large amounts. The maximum acceptable risk (figure B-3) also shows some patterns. It can be seen that there is a slight upwards patterns when the acceptable risk is set low. This is also very logical since it would mean that organisations will attempt to mitigate risk until it is absolutely 0. Thus over time they will keep increasing their budget, allowing them to invest more. The figure showing the effect for the minimum asset value (figure B-4) shows that a low asset value leads to a lower cyber security in the beginning. This can be explained by looking at the risk that a higher asset value brings with it. Thus for a lower asset value, organisations would have to have a lower cyber security level to reach acceptable values. However, over time their assets will grow and they will start upgrading their cyber security.

When looking at the global cyber security graphs, it can be said that the model is not very sensitive to the values of the parameters. This means that no unexpected effects will occur when parameters are varied. Furthermore, the behaviour that is shown is also expected and logical.

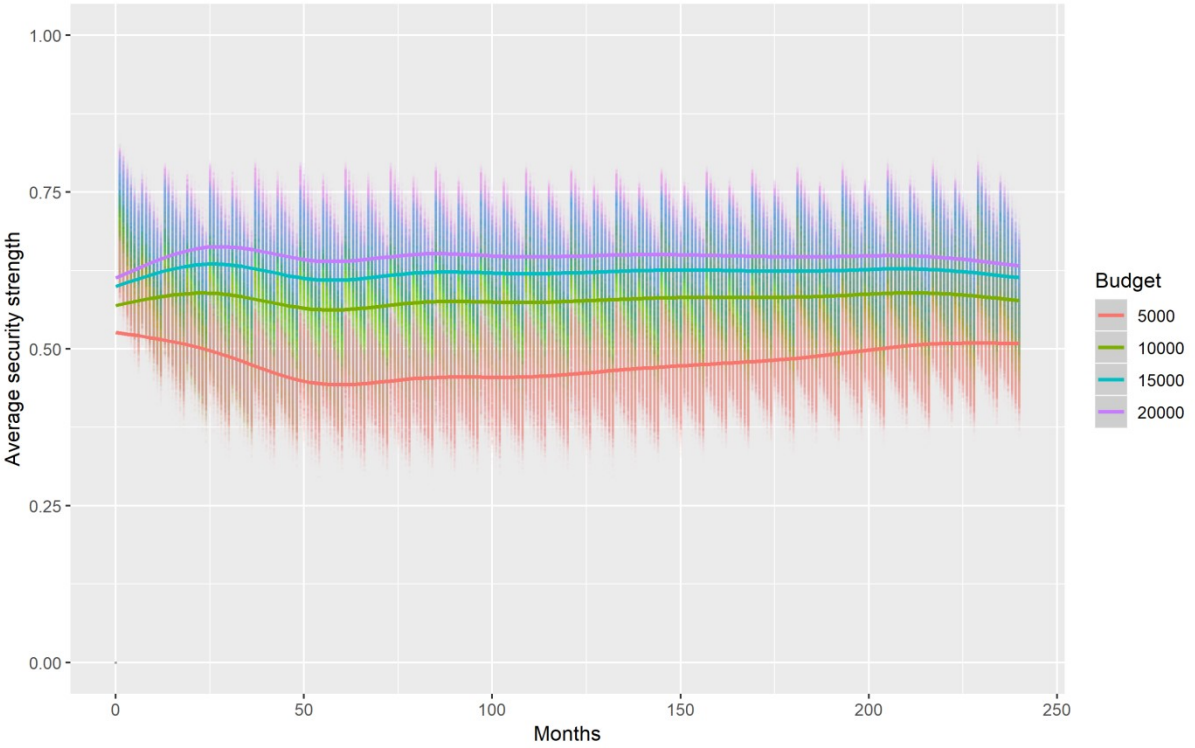

Figure B-1: The effect of organisation budget on the global cyber security strength

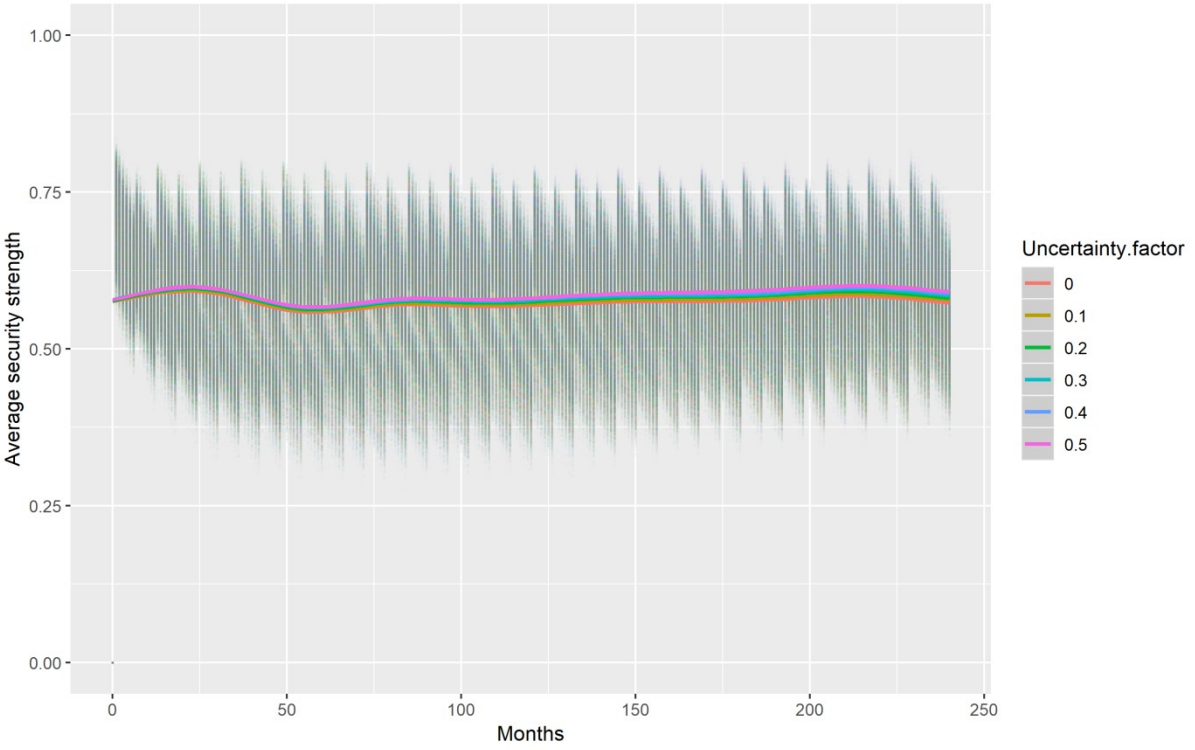

Figure B-2: The effect of assessment uncertainty on the global cyber security strength

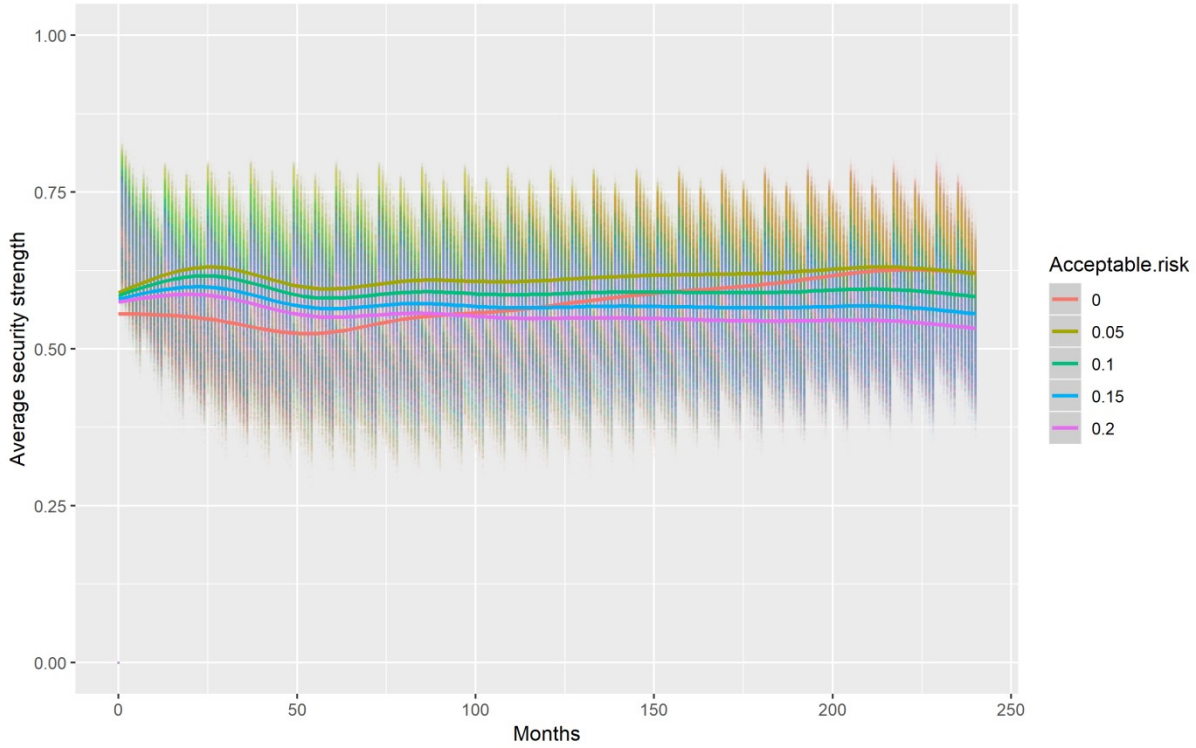

Figure B-3: The effect of maximum acceptable risk percentage on the global cyber security strength

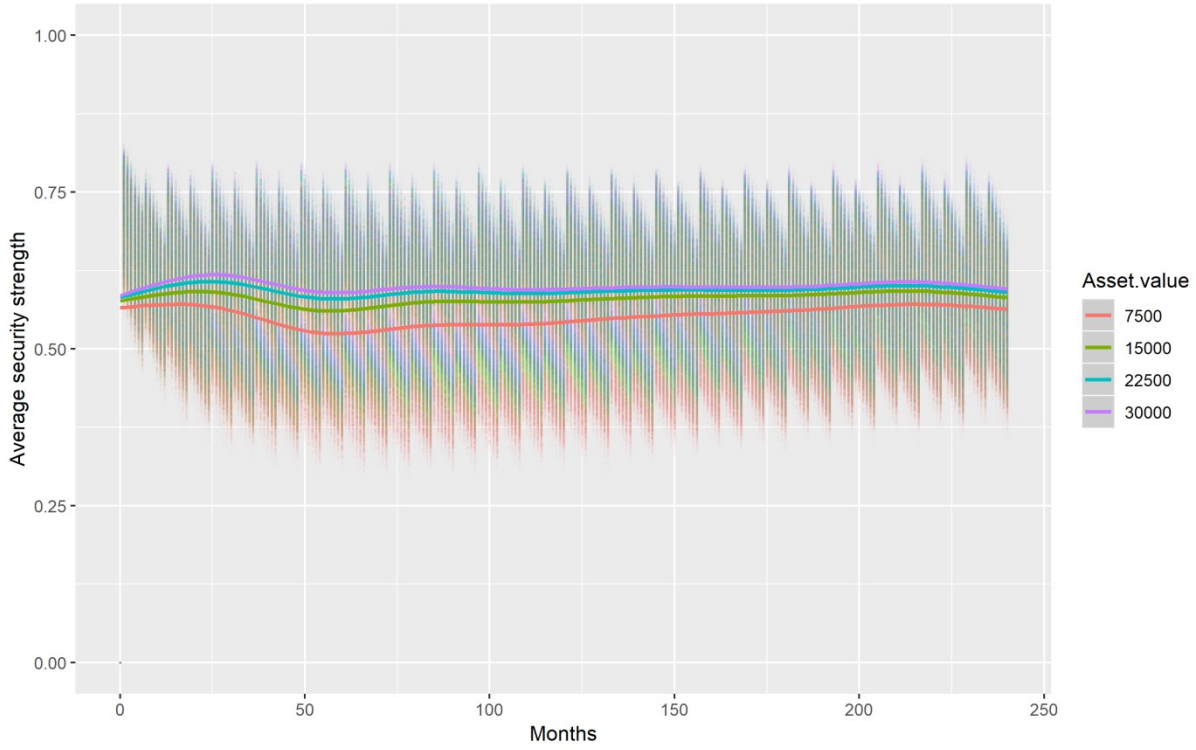

Figure B-4: The effect of minimum asset value on the global cyber security strength

Cyber security strength of insured organisations

The Figures for the analysis of cyber security strength of insured organisations is shown in figures B-5 – B-8. A first look at the figures shows similar behaviour to the global cyber security strength. This was expected since it measures the same value only specific to the insured organisations. However,

in the figures B-5 – B-8, a few data points can be seen at the bottom at value 0. These data points are caused by organisations deciding to start or stop buying insurance. This is expected behaviour since an organisation can change its decision based on the available budget or the risk they face.

The behaviour seen in the graphs is also very similar to the behaviour in the graphs of the global security. However, there are some subtle differences. For instance, a lower value for the maximum acceptable risk leads to organisations having nearly always higher cyber security strength. This is expected, since with 0% acceptable risk the organisations would invest maximally, thus a moral hazard would never occur. Another subtle difference is that there is more spread between the values of minimum asset value. This difference is caused by the coverage of an insurance package. An insurance package covers a certain amount, allowing organisations to only need insurance to reach an acceptable risk level. This is the case for lower asset values and also explains why the spread becomes smaller once higher asset values are used.

The graphs for cyber security of insured organisations also show that there is little sensitivity which is to be expected since the graphs are very similar to the graphs of the global cyber security strength.

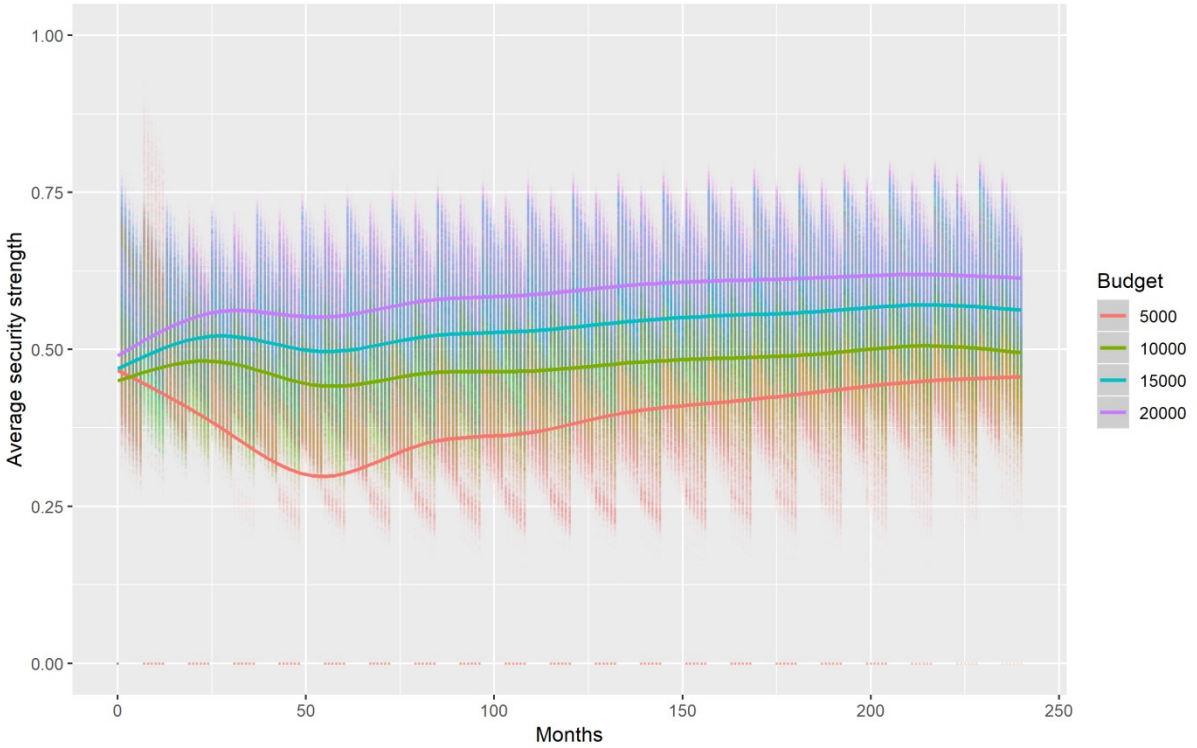

Figure B-5: The effect of organisation budget on the global insured cyber security strength

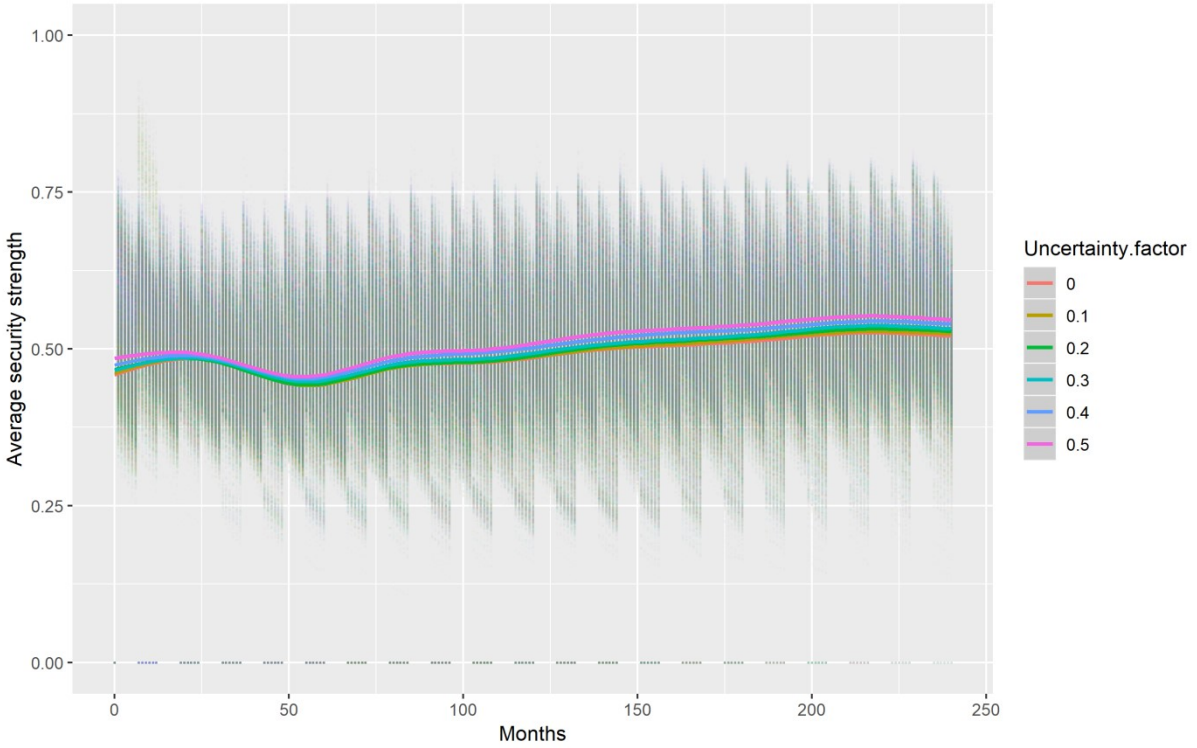

Figure B-6: The effect of assessment uncertainty on the global insured cyber security strength

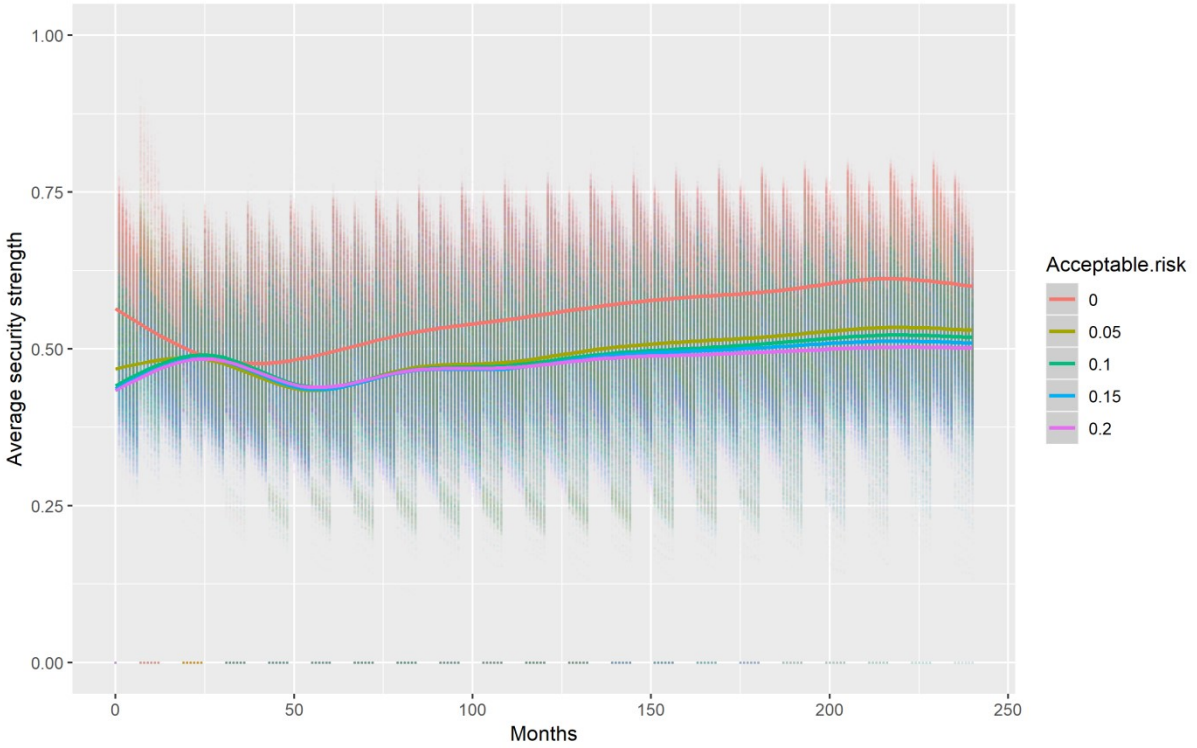

Figure B-7: The effect of maximum acceptable risk percentage on the global insured cyber security strength

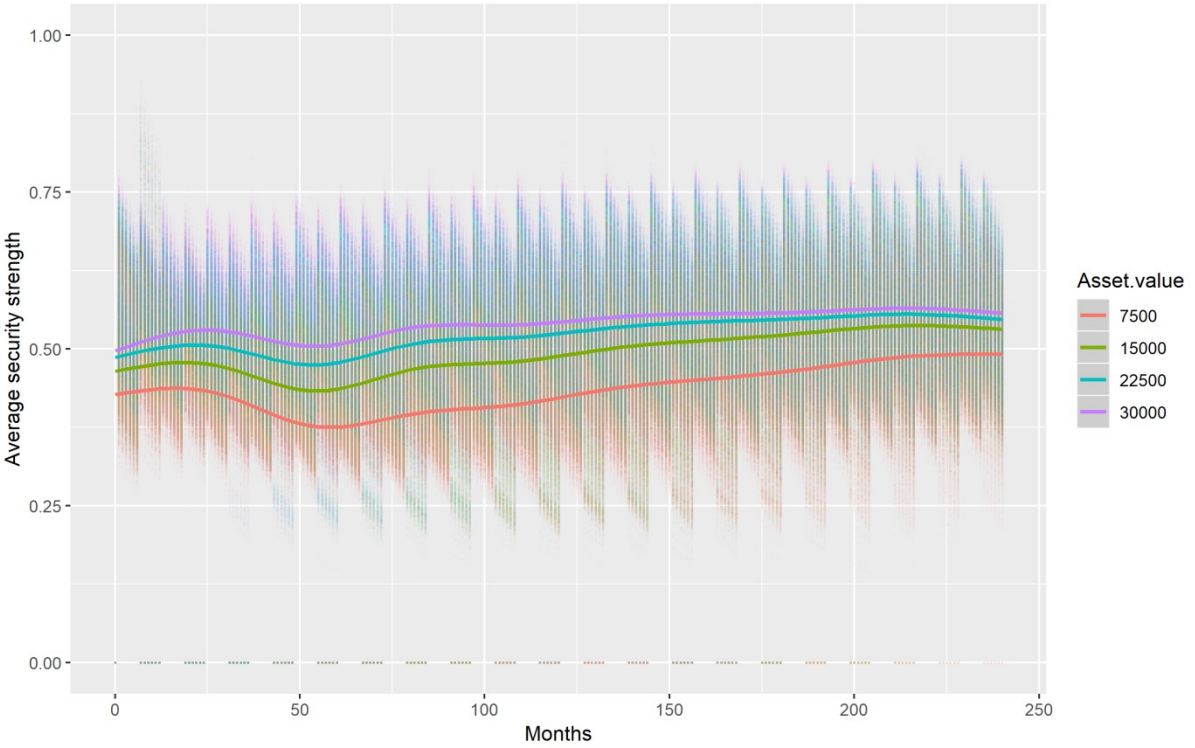

Figure B-8: The effect of minimum asset value on the global insured cyber security strength

Uninsured organisations cyber security strength

In figures B-9 – B-12 the graphs for the uninsured organisations are shown. These graphs show the same behaviour as the insured organisation graphs discussed above. As such, here too the data point at value 0 can be explained as being caused by organisations acquiring insurance and organisations choosing to only invest in their own security once their contract ends. The graphs for the uninsured organisations are very similar to the global cyber security and insured organisation cyber security graphs discussed above.

Since the graphs for the uninsured organisations are similar to the other graphs concerning cyber security strength, the conclusion is once again that there is little sensitivity to the parameters.

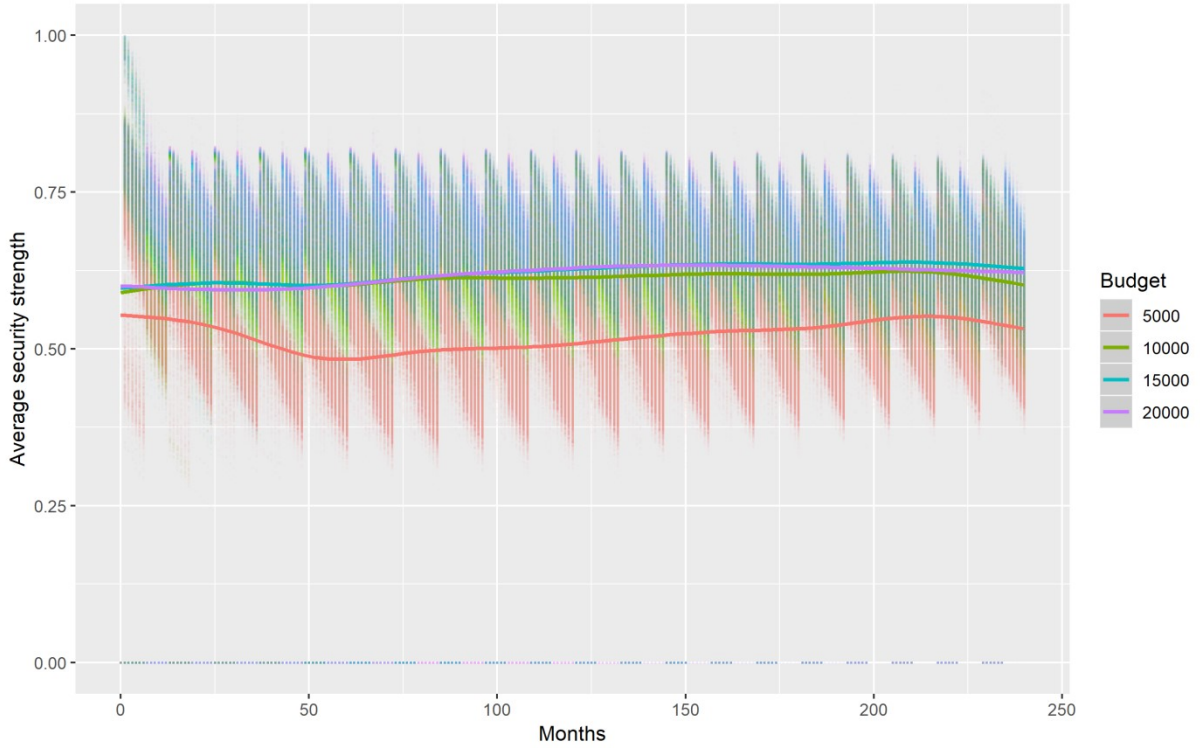

Figure B-9: The effect of organisation budget on the global uninsured cyber security strength

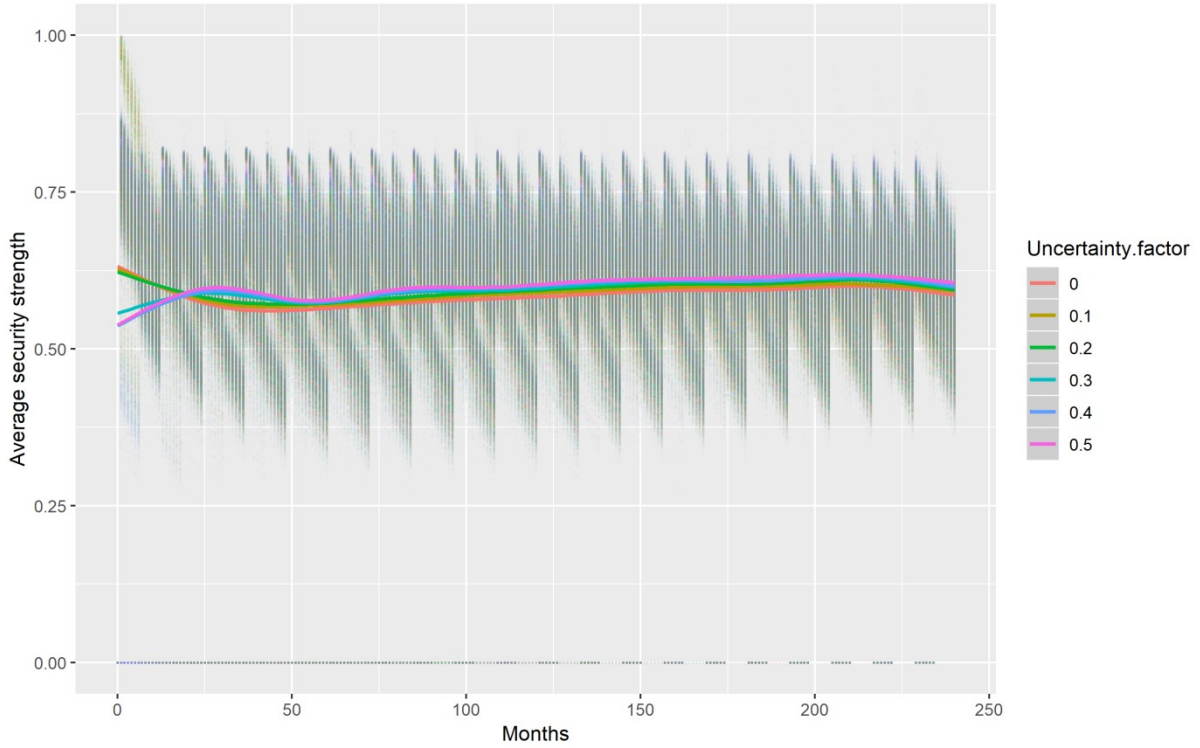

Figure B-10: The effect of assessment uncertainty on the global uninsured cyber security strength

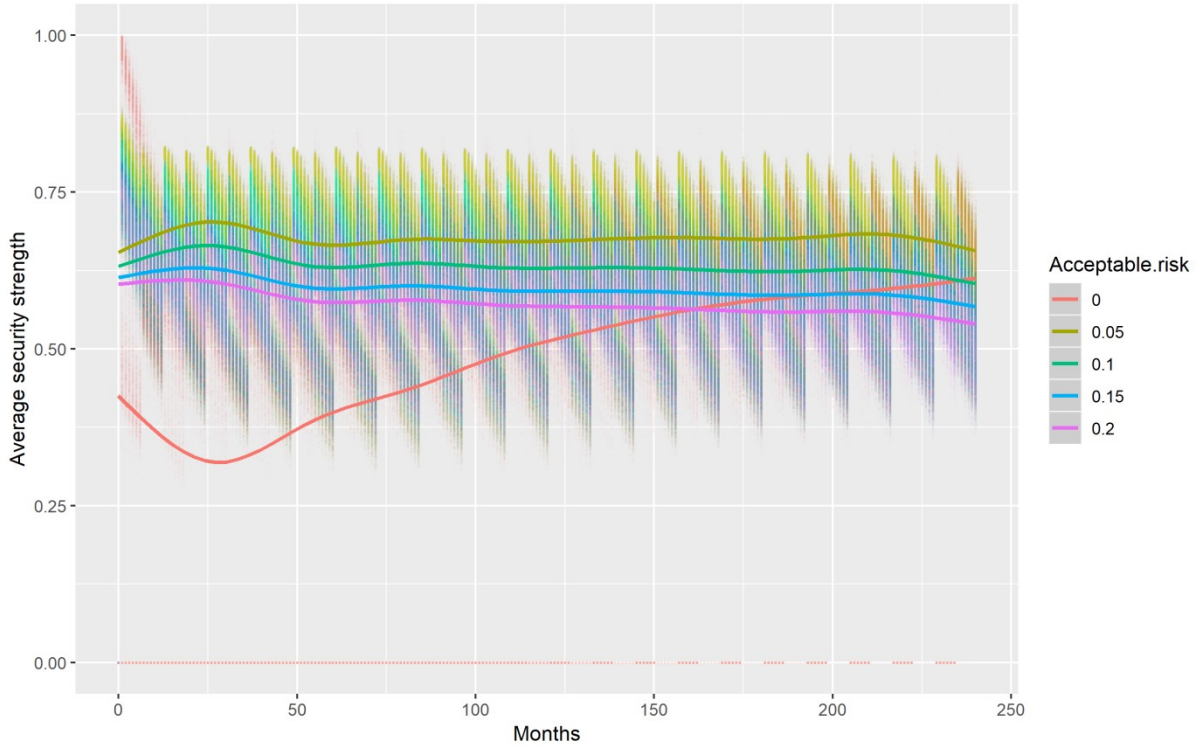

Figure B-11: The effect of maximum acceptable risk percentage on the global uninsured cyber security strength

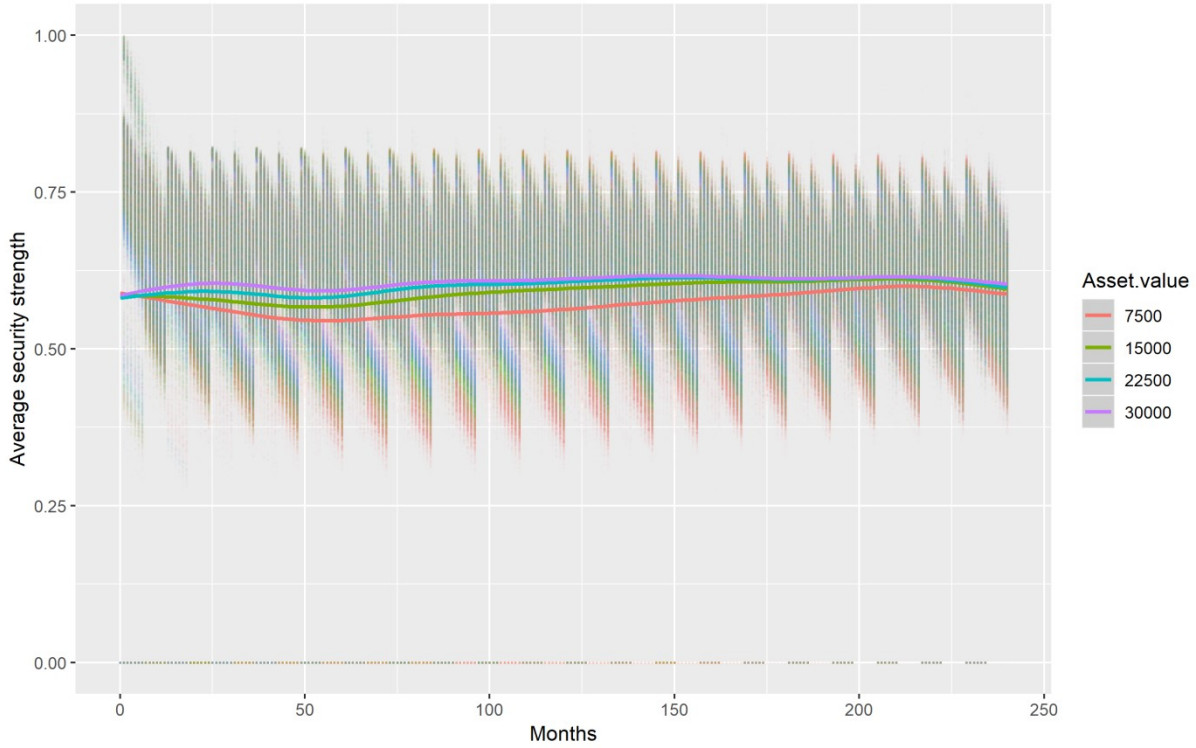

Figure B-12: The effect of minimum asset value on the global uninsured cyber security strength

Total annual budget

Organisations allocate budget for cyber security investments each year. The budget allocated is measured using the total annual budget. This metrics gives insight into the budget that is available to organisations and can show whether organisations have increased or decreased their budget as a

result of the risk they face. The sensitivity of the budget for the parameters can be interesting to analyse since this annual value is tied to the expenditure on cyber security controls and thus influences all other parameters.

The plots for the total annual budget are shown in figures B-13 – B-16. The first thing to note about the graphs is that there is quite a bit of chaos (a lot of spread). However, this is to be expected since the organisation budget was varied for the sensitivity analysis. Taking a closer look at the graph of the organisation budget in figure B-13, there is a clear distinction visible between the values used for the organisations budget. In the graphs it is clearly visible that lower organisation budgets rise over time whilst higher budgets decrease. This is because, depending on the situation, organisations will lower their annual budget if they don't use much of it. This effect can be seen in figure B-15 which contains the analysis of the maximum acceptable risk. A clear distinction is visible again, with higher values leading to lower annual budgets and lower acceptable risk causing the annual budget to grow. The assessment uncertainty and minimum asset value show little distinction. For these parameters it is likely that they are partly the cause of the chaos that is observable in the graphs. The spread in the figures can also be explained through the differences between organisations and their behaviour. Organisations all face a different amount of risk and have a different budget, this leads to larger or smaller decreases to the annual budget depending on whether they are able to mitigate enough risk with their budget.

The behaviour observed is all logical and expected. There is sensitivity to the organisation budget but this was to be expected since it is directly related to the annual budget. The maximum acceptable risk also proves to have an effect which is logical. Therefore, the sensitivity should not be problematic for experimentation.

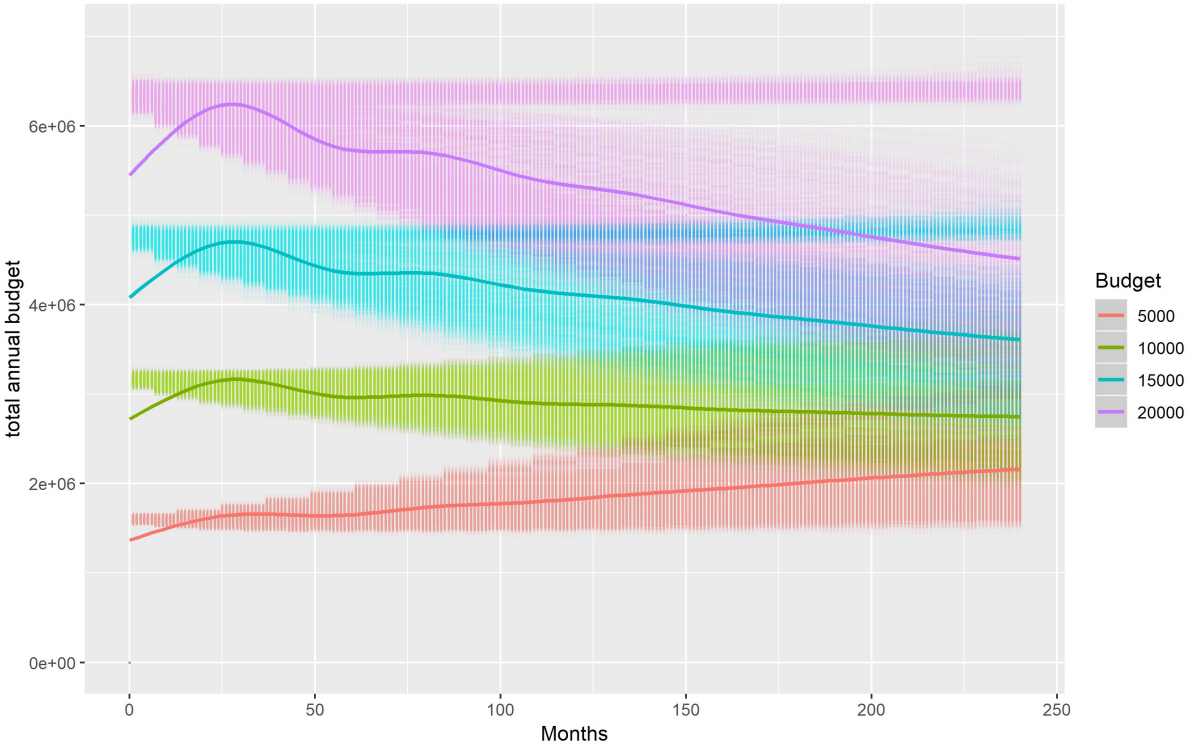

Figure B-13: The effect of organisation budget on the total annual budget

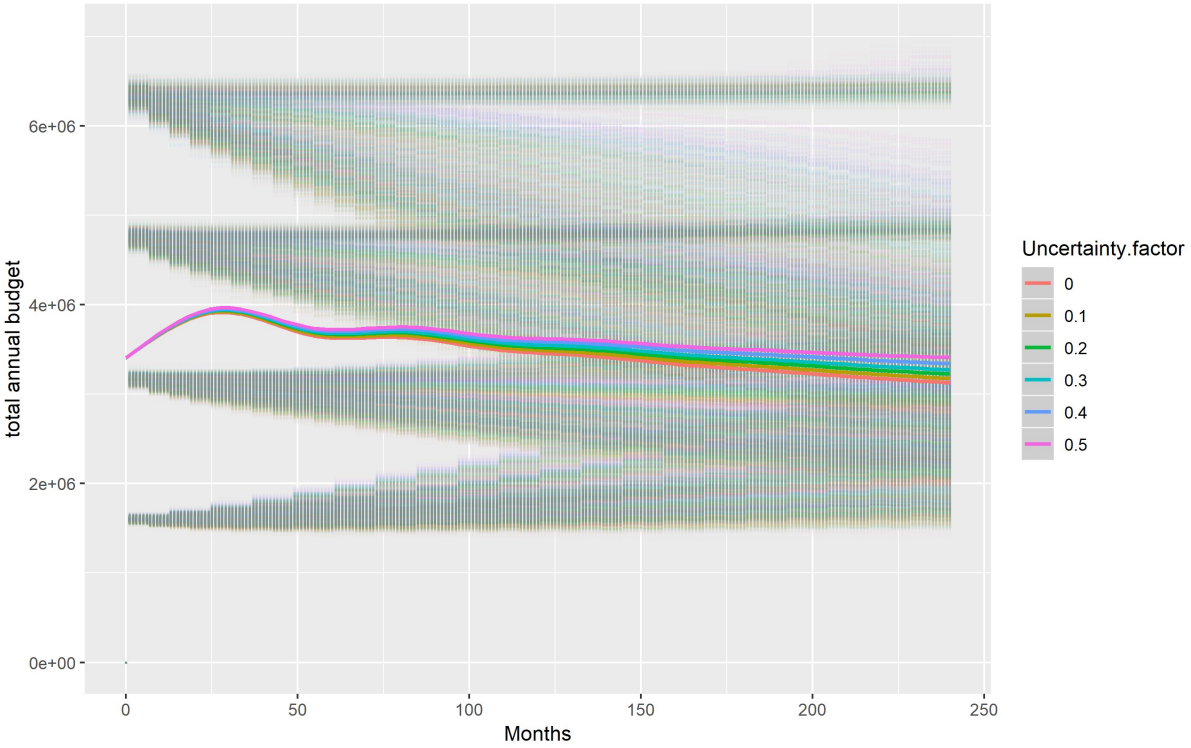

Figure B-14: The effect of assessment uncertainty on the total annual budget

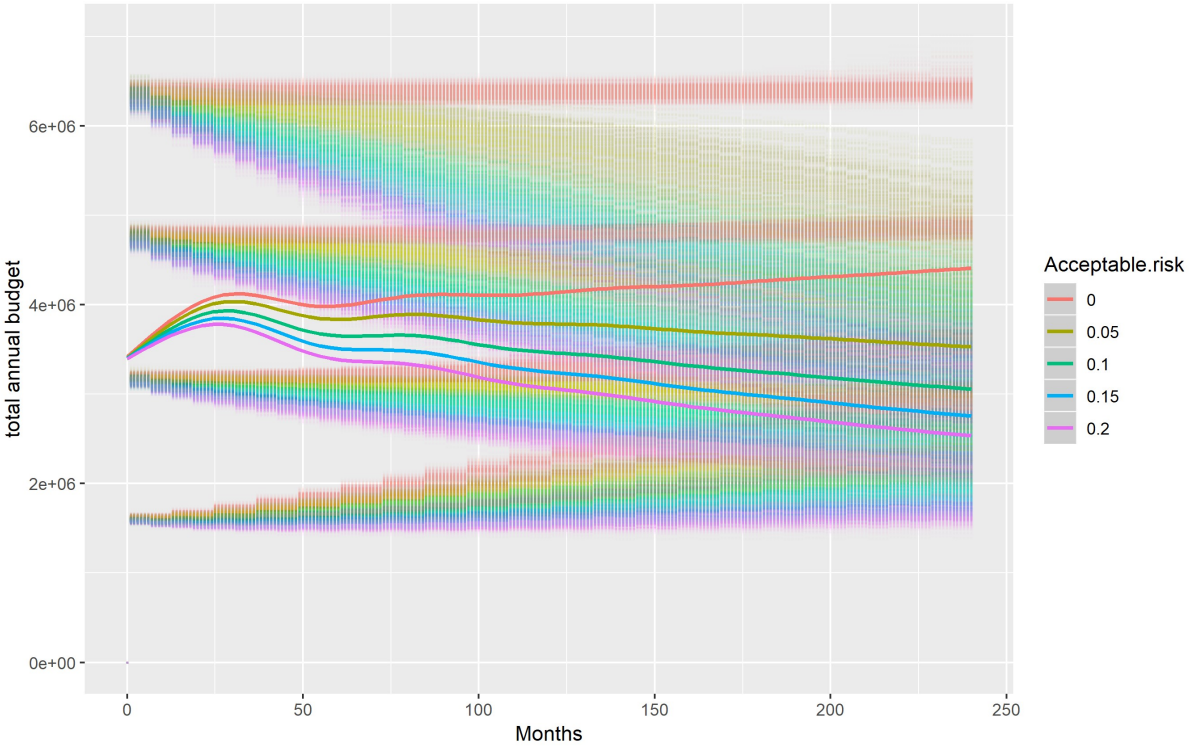

Figure B-15: The effect of maximum acceptable risk percentage on the total annual budget

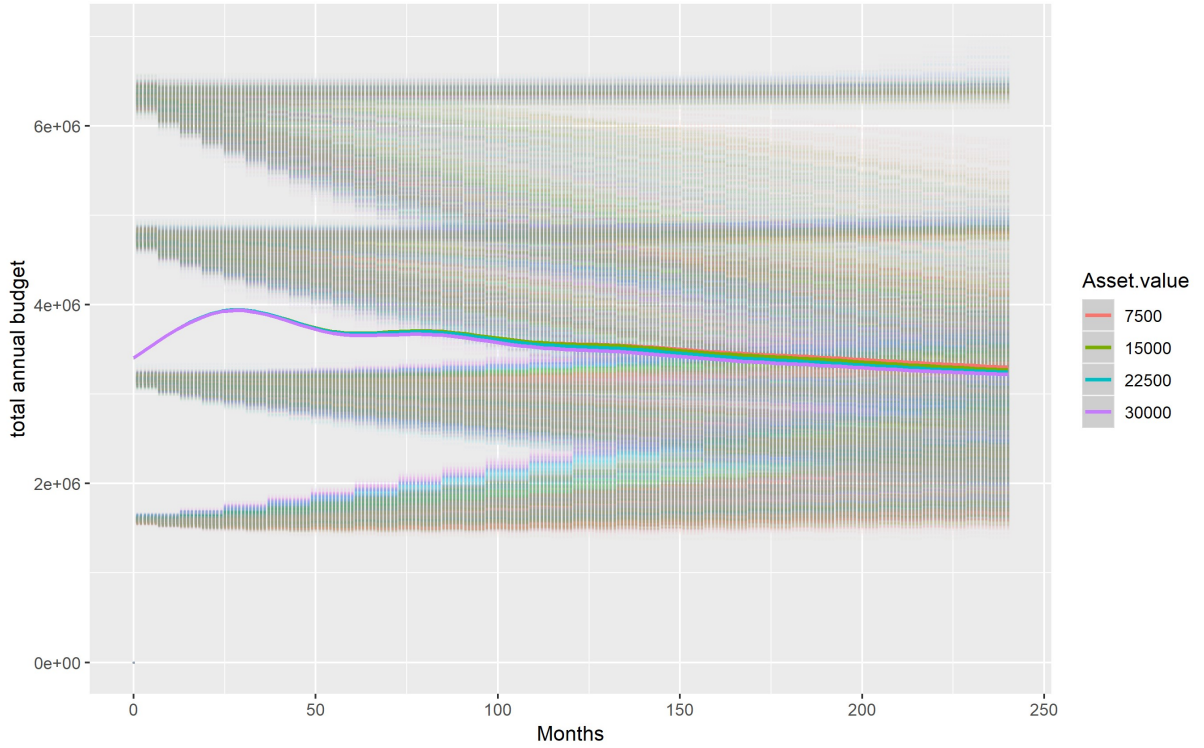

Figure B-16: The effect of minimum asset value on the total annual budget

Global value loss

The global value loss shows how much value is stolen over time. This metric is interesting for analysing the sensitivity since it keeps track of the most important value in the cyber security ecosystem. Organisations want to have as little losses as possible, which is why they concern themselves with CRM in the first place. Thus having a low value means that the organisations are effectively defending themselves against attackers. This is also of interest to insurance firms since they would want the losses to be as low as possible as well. Therefore, analysing the sensitivity of the global value loss for different parameters is important since the experiments will be focussed on influencing this metric among others.

In figures B-17 – B-20 the value loss for the four parameters is shown. The effect of the budget of organisations shows that for a low value there are slightly more losses for organisations. This is not surprising since the budget is directly related to the power an organisation has to reduce its risk because they have less money to invest. The graph concerning maximum acceptable risk indicates that a low acceptable risk reduces losses, which is logical since it makes organisations invest more. Figure B-20 shows the effect of the minimum asset value on the global losses. In this graph a very clear distinction can be observed, for low asset values the losses are low and vice versa. This is not unexpected since the asset values relates to the amount that can be stolen by attackers. There is also some spread observable in this graph. This can be attributed to the additional value organisations can have because of the mechanisms to create heterogeneity between organisations.

There is more sensitivity to the parameters observable when looking at the global value loss of organisations. The organisation budget appears to have a relatively low effect but the minimum asset value has a larger effect. However, this sensitivity is logical and expected and thus does not pose a problem for model experimentation.

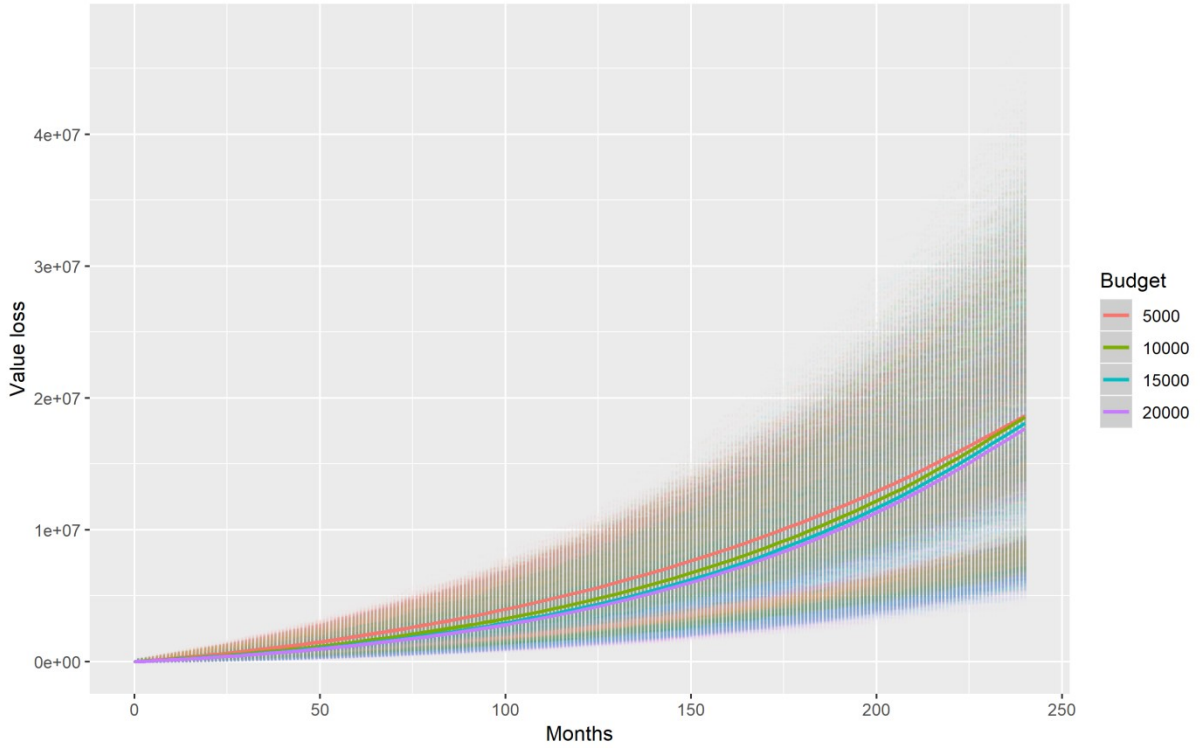

Figure B-17: The effect of organisation budget on the global value loss

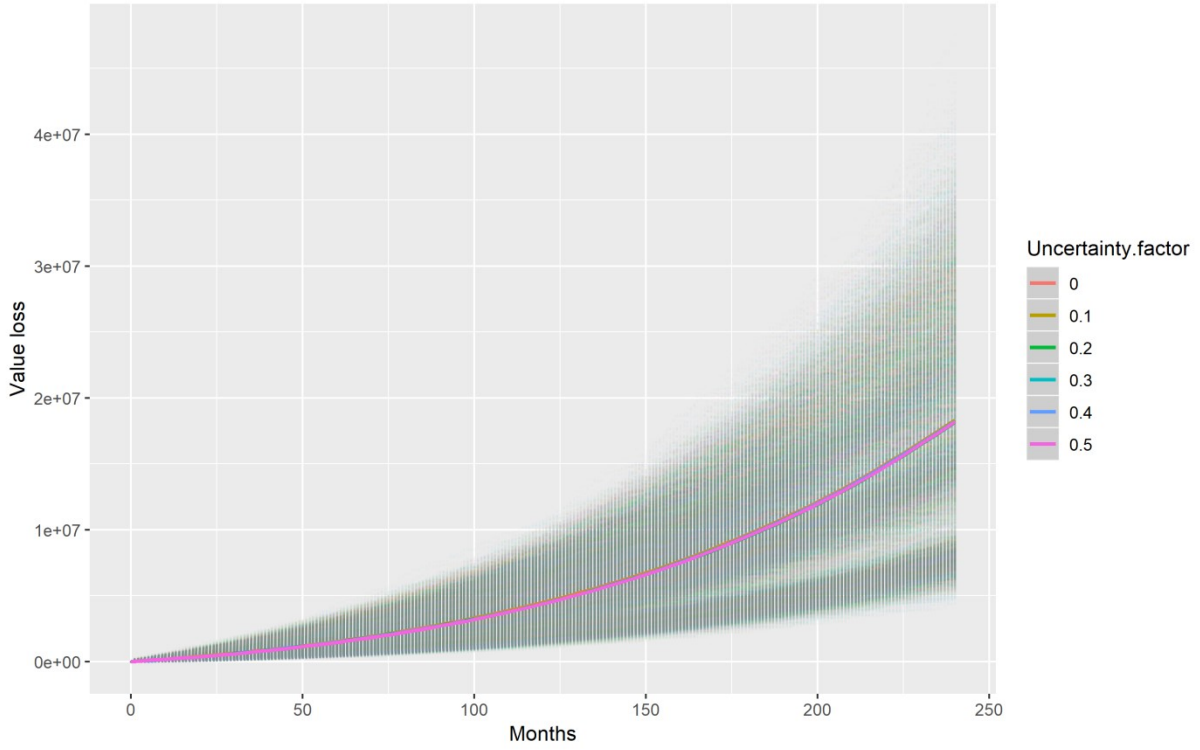

Figure B-18: The effect of assessment uncertainty on the global value loss

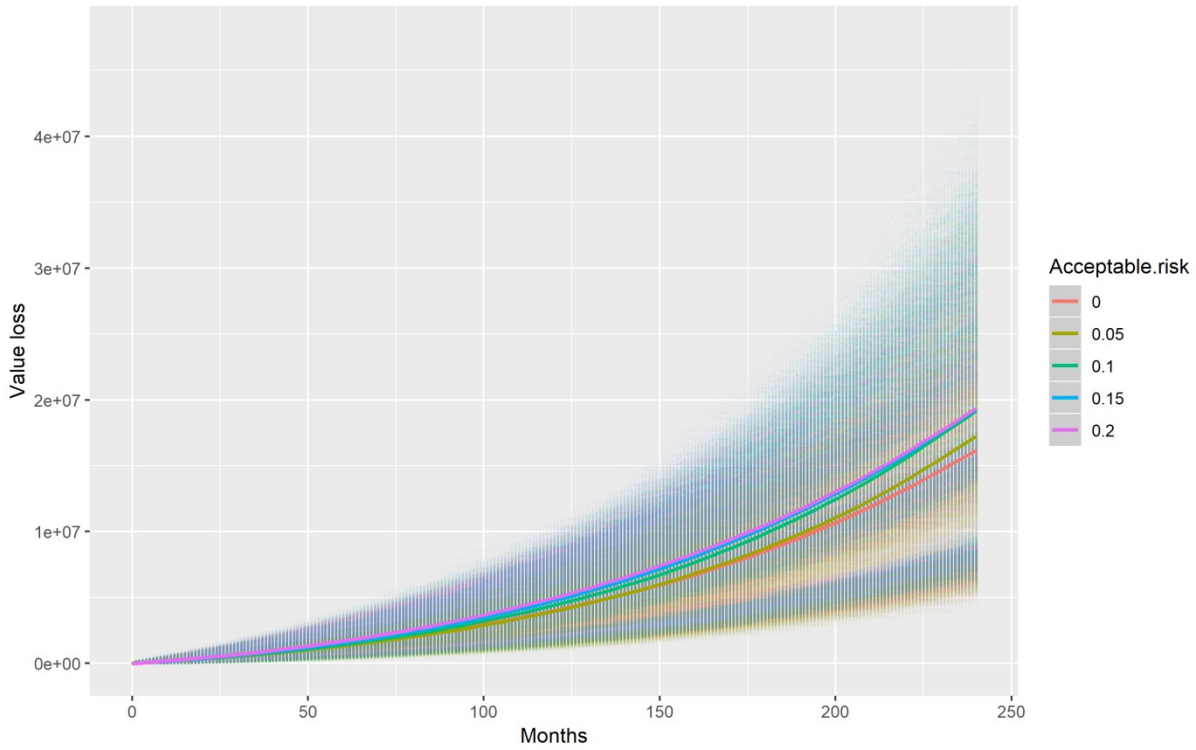

Figure B-19: The effect of maximum acceptable risk percentage on the global value loss

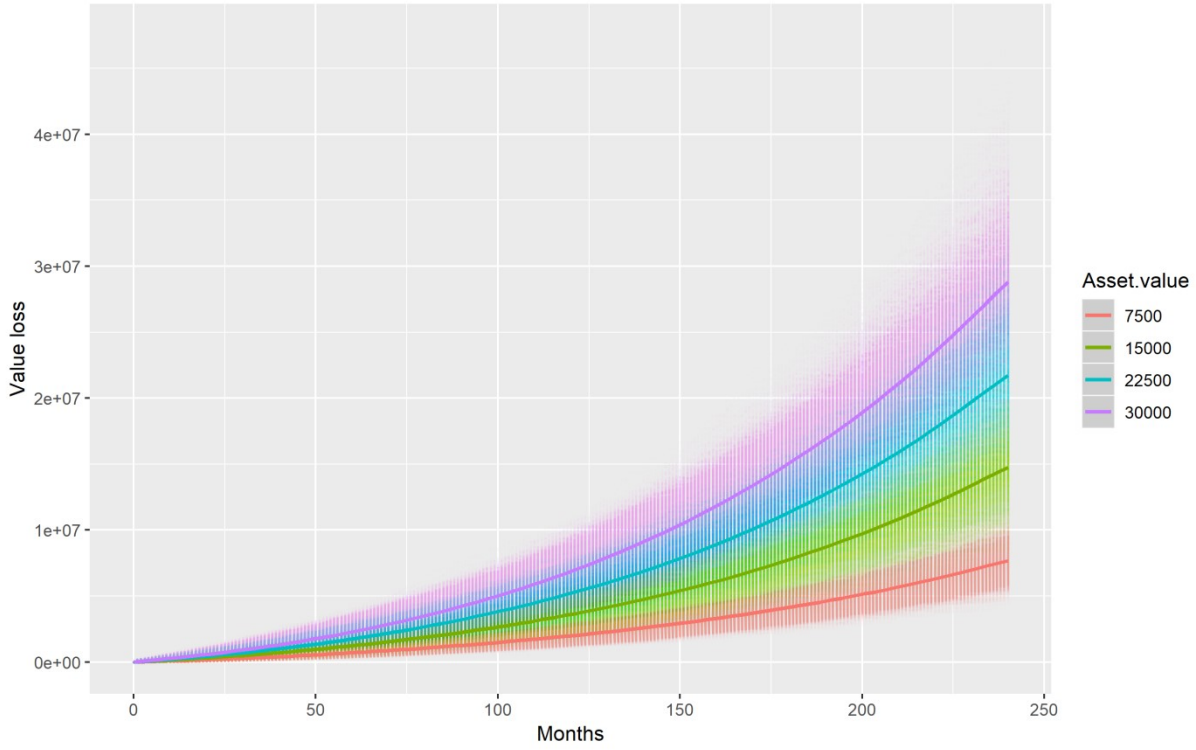

Figure B-20: The effect of minimum asset value on the global value loss