The influence of cyber insurance policies on the cyber security ecosystem

Jhoties Sewnandan
Delft University of Technology
Delft, the Netherlands

Abstract
Cyberattacks are a constant threat to organisations worldwide. The uncertainty and difficulty of properly conducting cyber risk management processes do not make it easier for organisations to cope with cyberattacks. Cyber insurance can be a partial solution to the dilemma that organisations face. However, it has not seen the expected growth which is likely because the actual effects of cyber insurance are still unclear. Furthermore, barely any literature is available on the insurance policies that insurers can utilise to positively influence the ecosystem. Additionally, the researches in current literature, whilst providing useful insights, still lack the chaos, interconnectedness and unpredictability (dynamicity) that characterises the cyber security ecosystem. In order to close this knowledge gap and tackle the issue of dynamicity, a modelling study was conducted utilising agent-based modelling. The agent-based model was built to simulate the cyber security ecosystem and to test the effects of various cyber insurance policies. The main findings from this research were that the various insurance policy options had positive but rather small influences. The combination of several policy options into a synergetic design provided results with more observable effects on ecosystem level. However, altogether there were still no large positive effects brought forth by the insurance policies on the cyber security ecosystem.

Keywords: Cyber insurance, Cyber security, Insurance policies, Policy synergies, Complex adaptive systems, Agent-based modelling

1. Introduction

Many investments are made into cyber security worldwide, in 2016 alone the amount of money invested was $81.6 billion (Gartner, 2016). The high amount is also no surprise since being breached can be devastating to an organisation. Organisations usually lose money but a breach can also affect their productivity and image or the attacker can steal other things like intellectual property or customer data. In order to mitigate this risk, organisations go through a process called cyber risk management. In this process the organisation assesses its risk and determines what controls to buy in order to reduce risk. However, assessing the state of cyber security, and thus the risk, is difficult and involves a lot of uncertainty. Furthermore, determining what controls to invest in is also difficult since there are many controls available and their actual effectiveness is unknown. As such, one of the options that an organisation can invest in is cyber insurance. The main advantage over investing in controls is that it provides certainty in the form of a specified coverage and premium. Additionally, perfect security is not possible, since vulnerabilities in controls are continually found and attackers continue to evolve as well as the tools they employ. Therefore, cyber insurance can be used to cover the residual risk as well.

However, the actual effects of cyber insurance on organisations and also on the cyber security ecosystem are still largely unknown. In particular one issue with cyber insurance is whether it influences the behaviour of organisations when it comes to investing in cyber security. There is a possibility that organisations have to split their cyber security budget to pay for insurance, leaving less money that can be used to invest in cyber security with (Gordon, Loeb, & Sohail, 2003; Pal &

Golubchik, 2010; Zhao, Xue, & Whinston, 2013). Furthermore, there is a possibility that organisations stop investing entirely since their risk has been covered by insurance (moral hazard). Another interesting question is whether cyber insurance can influence the cyber security ecosystem in a positive sense through its insurance policies.

Reviewing the available literature confirms the uncertainty on the effects of cyber insurance. Different opinions are expressed on whether cyber insurance is beneficial to the ecosystem (Bolot & Lelarge, 2009; Pal, Golubchik, Psounis, & Hui, 2014; Shetty, Schwartz, Felegyhazi, & Walrand, 2010; Yang & Lui, 2014). Furthermore, the literature on the effects of cyber insurance falls short in several ways. First the literature has focussed only on the direct effects of cyber insurance. This does not take into account how it could indirectly affect the ecosystem. For instance, a large amount of research has been done on the usefulness of cyber insurance to mitigate risk in organisations (Böhme, 2010; Gordon et al., 2003). Whilst it is useful to know why it is beneficial, the effect it has on how often it will be targeted as a result are not considered. Second, there is some literature available on the effects of cyber insurance, however, these studies have mostly used conceptual and mathematical model in order to analyse the system (Pal & Golubchik, 2010; Pal et al., 2014; Yang & Lui, 2014). These studies are missing the dynamic nature (chaos, interconnectivity and unpredictability that are part the ecosystem) and the interactions that define the cyber security ecosystem. Therefore, the results are still lacking in the insight that is obtained. Third, in literature there tends to be a focus on single entities at time when studying the effects of cyber insurance (Bandyopadhyay, Mookerjee, & Rao, 2009; Zhao et al., 2013). These studies provide valuable insight, but lack the interactions that define the cyber security ecosystem. Fourth, in literature very little attention has been paid towards the influence that insurance policies utilised by insurance firms could have on the ecosystem. These policies could be critical to ensuring that cyber insurance is beneficial to the ecosystem.

This study seeks to address the lack of dynamicity in literature through a simulation model of the ecosystem. Furthermore, this study intends to clarify some of the uncertainties on the influence that cyber insurance has on the ecosystem. In particular the focus will be put on the influence that insurance firms can bring forth through their insurance policies. The following research objectives have been formulated in order to address the knowledge gap.

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.

In this study the cyber security ecosystem will be simulated through agent-based modelling (ABM) in order to create a dynamic model of the cyber security ecosystem. The research question has been formulated as:

How do various cyber insurance policies influence the cyber security ecosystem?

This paper will follow the following structure: in section 2 the related work will be discussed. Section 3 will describe the concepts of the cyber security ecosystem which includes the behaviours and interactions of the actors in the system. The operationalisation of the model will be presented in section 4. Section 5 will provide information on the usage of the model and the results generated through its use. Section 6 will contain the conclusion and discussion.

2. Related work

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 organisations aren'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, Martinelli, Nanni, Orlando, & Yautsiukhin, 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.

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. However, data symmetry is not realistic for the time being since organisations tend to be secretive of their data concerning cyber security. In the end, there is still a need to obtain more insight into the influences of cyber insurance and to explore what is possible to positively influence the cyber security ecosystem.

3. Cyber security ecosystem behaviour and interactions

In order to understand the influence that cyber insurance can have and to understand what elements are important to modelling the ecosystem, it is necessary to identify and determine the concepts that define the cyber security ecosystem. In current literature most of the elements and concepts that make up the cyber security ecosystem have been thoroughly researched. Therefore, the concepts necessary to understand and model the system can be identified and described by going over the literature written on each element. The concepts that have been identified will be described below.

The cyber security ecosystem consists of three actors: organisations, attackers and insurance firms. The main interaction occurs between organisations and attackers. During this interaction, attackers attempt to breach the cyber security controls employed by the organisation. If the attacker is successful the organisation will lose assets to the attacker. Another interaction occurs between the insurance firms and organisations. This interaction is starts with an organisation performing its cyber risk management process. During this process the organisation will assess its risk and evaluate its options. In this process the organisation can consider buying insurance. The insurance firm will calculate a custom premium for the organisation in this interaction after which the organisation can decide to make a contract if the investment is worth it. The last interaction is also between insurance firm and organisation. This interaction occurs when an insured organisation is breached. The organisation will make a claim on its insurance contract. This will cause the insurer to assess damages and losses and pay out the value it assessed. These interactions can be seen in figure 1 which shows the conceptual model of the ecosystem.

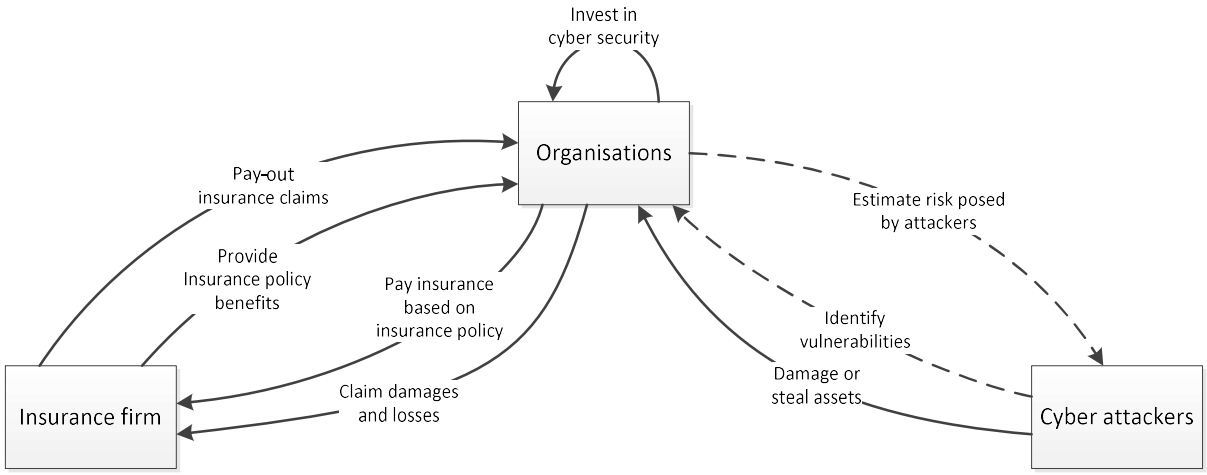

Figure 1: Conceptual model of the cyber ecosystem

A system is defined by the actors and their interactions with each other (Van Dam, Nikolic, & Lukszo, 2013). Therefore, in order to truly understand the system, it is necessary to understand the behaviour of the actors. This will make it possible to understand how the system as a whole behaves as it does as well. Below, the concepts for each individual actor will be discussed.

3.1 Organisations

The core of every organisation is to make a profit. In order to make a profit, organisations perform various activities which generate assets that can be leveraged to their advantage (DeAngelo & Roll, 2015; Dowling, 1993). It is because of these assets that organisations become targets of people with ill intentions. The increase in connectivity has also played a part in the increase in cyberattack (Ögüt et al., 2011). Cyberattacks carry very little risk for attackers because they are hard to track and hackers don't have to be physically present (Nykodym, Taylor, & Vilela, 2005).

In order to handle the increased risk to their assets, organisation started conducting cyber risk management (CRM) processes to protect their assets. Cavusoglu, Mishra & Raghunathan (2004) define 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. This implies that CRM is all about striking a balance between investments in cyber security and the savings that result from it. However, striking this balance can be difficult because of uncertainty and lack of information. Still organisations have little choice but to invest into their cyber security which encompasses many different controls that can be used to defend against cyberattacks (Von Solms & Van Niekerk, 2013). It is for this reason that investing in cyber security is also difficult because there are many factors that need to be considered and there is a large array of controls available (Cavusoglu et al., 2004). However, it is still impossible to reduce the risk to zero since the landscape is continually changing and evolving (Marble et al., 2015; Rowe & Gallaher, 2006). Therefore, organisations make use of an acceptable risk value. This is the point where the organisation determines that investing more money will actually reduce their gains in the end as it is not worth the investment (Hausken, 2006; Salter, Saydjari, Schneier, & Wallner, 1998). This is a good thing because security investments also become less effective at higher levels of investments (Moitra & Konda, 2000).

Cyber insurance can provide more certainty in cyber security because organisations know exactly how much risk can be averted through it and a fixed price is paid (Gordon et al., 2003). However, insurance can cover the risk to great extent, possibly giving rise to a moral hazard because organisations do not have to invest their complete budget anymore (Hoang, Wang, Niyato, & Hossain, 2017). As a result of insurance, organisations can end up with lower security and get attacked more often. However, since insurance will cover most if not all costs, the organisation is still better off financially.

3.2 Attackers

There are many different types of attackers. Each attacker has a certain motivation that drives them to attack an organisation for it. The motivations can range from wanting money to wanting to obtain intellectual property or wanting to do damage (Rosenquist, 2009). Furthermore, attackers also have different skills and resources available which can make them very diverse and thus difficult to defend against. Organisations have found a way of dealing with this through, what is called, attacker profiles. Attacker profiles are used to classify attackers based on various characteristic that are deemed important by an organisation (Nostro, Ceccarelli, Bondavalli, & Brancati, 2014; Nykodym et al., 2005). These attacker profiles allow organisations to focus on attackers that are most likely to attack thus allowing organisations to make specific investments. However, besides attackers themselves, the tools they can use are also very diverse in the effectiveness, deployment and rarity to name a few examples. This further increases the difficulty of defending against cyber attackers.

3.3 Insurance firms

Insurance firms provide insurance and takes on the risk of an organisation in exchange for fixed continual payments (Bolot & Lelarge, 2009). This gives organisations more certainty about their cyber security and the risk they face. However, insurance firms are also organisations themselves meaning that they are also out to make a profit. The product that insurance firms sell is risk displacement, for which they use insurance policies to state the conditions. The premium that is asked by insurance firms is custom calculated for each specific organisation as to reflect the risk that they will take on by entering into a contract (Innerhofer-Oberperfler & Breu, 2010). This prevents the insurance firm from making a loss, since the amount of risk is compensated by higher payments. Several packages can be offered by insurance firms, where more complete packages are accompanied by higher premiums (Ögüt et al., 2011).

There are several other options that can be used by insurance firms in their insurance policies besides the premium price and coverage. For instance, they could differentiate between types of losses and cover only a few of them or require that organisations invest a certain amount of money into cyber security on a yearly basis.

Insurance firms do have to follow governmental policies in the design of their insurance policies. The policy maker creates governmental policies in order to regulate the market (Böhme, Schwartz, & others, 2010). This is done to ensure that the market can remain functioning and that nobody is victimised. The guidelines and policies created by the policy maker do not have to interfere with insurance policies necessarily. This is because the guidelines and policies are usually aimed more toward extreme cases that could end up doing harm. Thus insurance firms still have a lot of space left to design their insurance policies.

4. Operationalisation

The concepts discussed and presented in the previous section first have to be operationalised into the agent-based model before the influence of cyber insurance policies can be researched. Complex adaptive system thinking was utilised to facilitate the operationalisation of concepts into the agent-based model.

4.1 Complex adaptive systems

Complex adaptive systems (CAS) thinking was used for two reasons. The first reason is because it helps in understanding complex systems. The way of thinking that CAS describes help in understanding the components that make up the system thus gaining an understanding of the system itself. The second reason is because, by describing the cyber security ecosystem as a CAS, will make it possible to naturally model it into an ABM model. This is because ABM models are made by modelling the components that make up a system. This is the same way the system is decomposed and observed when using CAS thinking.

Holland (1992) explains that complex adaptive systems can be thought off as a system that exists out of multiple layers. It is because of the layers that the system shows particular emergent behaviour. The idea behind CAS is that the components in each layer are autonomous, capable of behaving, interacting and adapting according to its environment (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).

The cyber security ecosystem possesses these attributes, thus it can be said that it is a complex adaptive system.

4.2 Operationalisation of the agent-based model

In the light of CAS the model concepts were described in section 3. This makes it possible to operationalise the concepts as to create the agent-based model. The states and actions for each actor have been identified based on the concepts described in section 3. The states and actions are based on the behaviour of the actors and their interactions. These states and actions can be found in table 1.

Table 1: Actor states and behaviour

Actor	States	Actions
Organisations	Cyber security level, Budget, Size, Asset value, Recently attacked, Insurance contract	Conduct CRM processes, Buy insurance, Recover from cyberattacks, Increase / depreciate asset value
Attackers	Attacking, Attack profile, Tool	Select target, Attack organisation
Insurance firms	Premium per package, Coverage per package, Risk selection, Incentivisation, Upfront risk assessment, Sharing cyber security control information, Mandatory security level requirement, Obtaining premium payments	Determine custom premium, Pay-out insurance claims

The states and actions are used by the actors to interact with each other. The states depict the variables an actor has which influence its behaviour. For instance, recently attacked is a state with value true of false. If this is true then the organisation will behave in a certain way. Another example is the budget, this variable has a constant scale representing money. The budget is of effect on the steps an organisation can take to protect itself thus influencing its behaviour. The states and actions presented in table 1 will be used to simulate the each actor in the agent-based model. However, it is not possible to model all behavioural mechanisms of each actor since this would make the model too complex, thus increasing the development time and make the model slower to run. Therefore, several simplifying assumptions have been made to limit the complexity of the model. The mechanisms that were simplified were either too complex to model or deemed as having little effect on the outcome and could therefore be modelled in a simplified form or be left out altogether. In appendix A the simplifying assumptions have been described.

Based on the states and actions, the agent based model could be formalised and operationalised. The formalisation involves translating these states and actions to procedures that could be performed by a respective agent in the model. The operationalisation refers to the coding of the procedures in order to create a model that simulates the cyber security ecosystem. In appendix B and overview of the formalised model can be found.

5. Simulation model and results

In the previous section the operationalisation was described for the agent-based model. In order to make clear how the model exactly works, the model narrative will be discussed. Afterwards, the experimental design will be presented to make clear what insurance policy options were selected for experimentation. This will be followed by the results of the experiments.

5.1 Model narrative

The model narrative follows the overview of the formalised model procedures shown in appendix A. below a short model narrative will be given to clarify the procedures and their function.

The first step in the model is to setup the agents (actors) in the model. This provides all actors with their starting variables and values for these variables. In this procedure differences between agents are made. For instance, the amount of budget for each organisation is different within a specified boundary. The setup is only run once before the model runs are started. The procedures after the setup are part of the runs of the model and are performed each month in the model.

At the start of a run, the first procedure, *reduce cyber security effectiveness*, is performed. This procedure lowers the cyber security strength of organisation as to simulate vulnerabilities being

found, attackers becoming more skilled, new hacking tools being used, etc. Afterwards, the procedure to *update the status of organisations* is performed. This procedure is made up of several sub-procedures. Following the flow shown in the procedure, the organisations update their recovery timer, mutate their assets value, allocate cyber security budget, pay premiums and update contract duration. Once the organisations have updated their status, a main procedure, attack organisations, will be performed. In this procedure the attackers will choose a target, obtain a tool and attempt to attack the organisation targeted. When an attack has succeeded the attackers will also steal asset value. This can trigger the organisation to make a claim on insurance as well, if it is insured. The end of this procedure will start the next main procedure: *conduct CRM process*. In this procedure organisation assess the risk they face and determine what options it has to mitigate risk. This could involve the insurance firm, who is asked to calculate a premium price for each package. If the organisation determines that insurance is the best way to go, it will also make a contract with the insurance firm for the calculated insurance premium and specified coverage.

5.2 Experimental design

In this study the goal is to research the influence that various cyber insurance policies can have on the cyber security ecosystem. Therefore, the experimental design is focussed on exploring the effects that policy options have. This implies that the general parameters in the model will have to be kept constant in order to be able to test and compare the effect of the various policies to a baseline.

The baseline that was designed is shown in table 2. Because of a lack of concrete data, these values were chosen because they represent realistic values or because they created realistic patterns in the model. The values were assessed by performing a sensitivity analysis, which provided insight into the effects of several parameters on the behaviour in the system. By comparing the results of the sensitivity analysis to expected behaviour, values could be selected. Additionally, other values were chosen based on logical reasoning, for example, using a contract length of 12 months is logical since yearly contracts are commonly used in the business world.

Table 2: Experimentation baseline setup

Parameters	Value
Organisation-budget	8000
Assessment-uncertainty	0.2
Maximum-acceptable-risk-percentage	0.1
Minimum-asset-value	20000
Assets-variance	0.5
#Large-organisations	40
#Medium-organisations	50
#Small-organisations	35
#thiefs	50
#spies	35
#professional-hackers	25
#activists	20
Contract-length	12
Pay-out-factor	0.95
Insurance-package-1-coverage	7500
Insurance-package-1-baseprice	4000
Insurance-package-2-coverage	11000
Insurance-package-2-baseprice	6250
Insurance-package-3-coverage	15000
Insurance-package-3-baseprice	8000

Several policy options were identified and have been used for the experimental design. However, it is not possible to experiment with all possible values for these options since this would make experimentation take too long. Therefore, a selection of values has been made for each experimentation parameter that can have multiple values. The selected values were chosen because it is likely that these values would explore the full range of influence that an experiment parameter can have whilst still being realistic. Thus, it is likely that these values will provide the most interesting results. The options that have been selected for the experimental design are:

- Package options
- Contract length
- Risk selection
- Incentivisation
- Upfront risk assessment
- Sharing cyber security control information
- Requiring organisations to maintain their security level

The insurance policy options and the values that will be used for experimentation are discussed below.

Insurance package options

The insurance package options are made up of two components: premium price and coverage. The package options consist of three packages that are offered to organisations. The selected values are shown in table 3.

Table 3: Premium price and coverage values for experimentation

	Premium price			Coverage		
Parameters	Setup 1	Setup 2	Setup 3	Setup 1	Setup 2	Setup 3
Insurance-package-1	2000	4000	8000	2500	7500	12500
Insurance-package-2	3125	6250	12500	6000	11000	16000
Insurance-package-3	4000	8000	16000	10000	15000	20000

The setup shows which values of the premium and coverage are offered to organisations. As can be seen in the columns of premium price, there are three setups, whereas each setup has a value for insurance packages 1, 2 and 3. This means that if setup 1 is used than the premium prices listed in that column will be used for the representative packages. The columns for the coverage work in the same way as the premium price. Therefore, setup 1 has a premium price and coverage for each insurance package. The values shown in table 3 were chosen because it includes the baseline variable (setup 2) and also has an upper and lower bound. By using this experiment, insight can be obtained on what happens when an insurance firms varies the most basic policy options it has, the coverage and premium.

Contract length

The contract length is considered for experimentation since it has shown to have varying effects on the behaviour of organisations. This is because it limits organisation choices when longer contracts are used. The values 6, 12 and 24 months will be used since they represent realistic contract lengths. It is unrealistic to use higher values since this would require more commitment of organisations which is unlikely in a system with a lot of uncertainty.

Risk selection

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. This could have varying effects on the ecosystem, thus it is interesting to experiment with. The values chosen for risk selection are 0, 0.25 and 0.5. These values were selected because it gives insight into how severe the effects are when the factor is changed. The factors represent a value of up to 25% increase in price and up to 50% which seem reasonable to test the influence.

Incentivisation

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. For this option the value can only be true or false.

Upfront risk assessment

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. The values for this experiment can be only true or false. The factor that is used for calculating the extra costs is 10% of the base premium price. This seems a reasonable amount since the price would be a fraction of the premium price but wouldn't scale with the custom premium.

Sharing cyber security control information

Insurance firms gain information from all the clients that have a contract with it. This information can be shared by the insurance firm to help organisations make better or more effective decisions (Biener, Eling, & Wirfs, 2015; Marotta et al., 2017). This value also makes use of a value of true or false.

Requiring organisations to maintain their security level

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. This parameter only has the values true and false.

5.3 Results

The experiments were performed using a full factorial approach. This means that all possible values of all parameters were experimented with. The experiment runs have been measured using: global security strength, security strength of insured organisations, global value loss, value loss of insured organisation and the number of insured organisations. The performance of the experiments on these metrics can be found in figure 2 to 6. For each run the baseline setup was used and only the parameter that was being tested was varied. Therefore, the effect of only that parameter could be highlighted and analysed. Furthermore, specific values are shown for insurance package option (setup 0), contract length (24) and risk selection (0.25). This was done to add at least one unique run for those parameters, otherwise they would default to the baseline. For the other experiments the run with the parameter set to true was plotted. The synergy experiment has the following parameters set outside the baseline values: contract length: 6, required security level: true, incentivisation: true, sharing control data: true

The figures shown below indicate different things on the performance of the experiments. Figure 2 shows the global security strength in the ecosystem. In this figure is can be seen that all runs

end up quite close to each other. However, the most important run to look at is the baseline since this serves as a benchmark for the other runs to compete against. Observing how the baseline run went, it is possible to see that only three runs have managed to increase the cyber security strength in the system. But when looking at figure 6 it becomes clear why these runs have managed this. The number of insured organisations is lower for all these runs. Therefore, it is logical that the security strength grew since there are fewer insured organisations. Insurance by itself has a negative effect on the ecosystem since it displaces risk for money but does not increase the cyber security strength of an organisation. Therefore, if there are more uninsured organisations, the average would move up. Thus figure 4 also needs to be considered since it shows the global value loss. In this figure it can be seen that the runs once again end up close to each other. It is also likely that the baseline is in the middle of the runs, meaning that the synergy experiment did indeed have a positive effect on the cyber security strength as well, although the effect was very small. The same pattern as the global security strength is shown in figure 3 for the insured organisation cyber security strength. However, in this graph the difference between the baseline and the synergy experiment, sharing insured data and upfront risk assessment has become larger (as well as risk selection but since there are only a select few insured organisations it will not be mentioned from here on). This means that there was a positive effect on the cyber security of insured organisations at least. Figure 5 shows a very wide spread between the different experiments. This can partly explained by looking at the number of insured organisations for each run. The other part is explained by the effect of the policy option itself. However, if the effect of fewer insured organisations is taken away it is still very likely that the differences would become very small. However, despite this, the synergy experiment is the best performing policy option compared to the other experiments. This is also not strange since the synergy experiment is based on policy options that already provided positive effects.

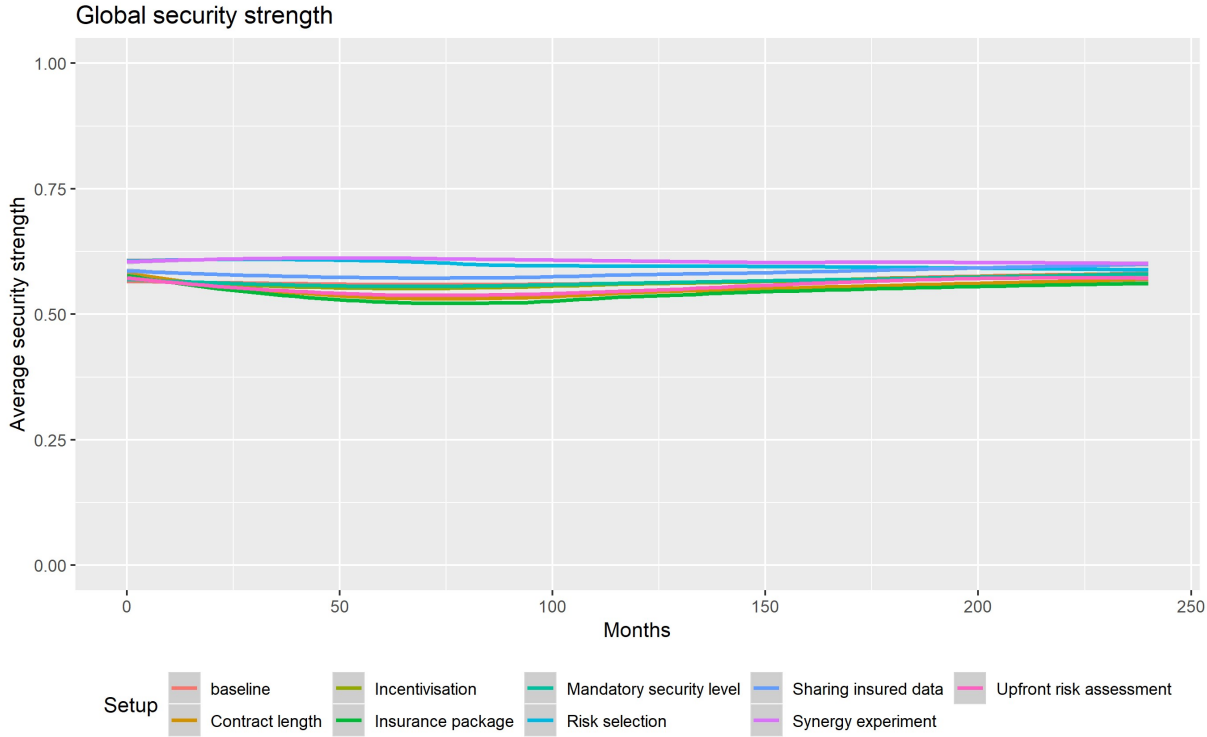

Figure 2: Experiment performance on global security strength

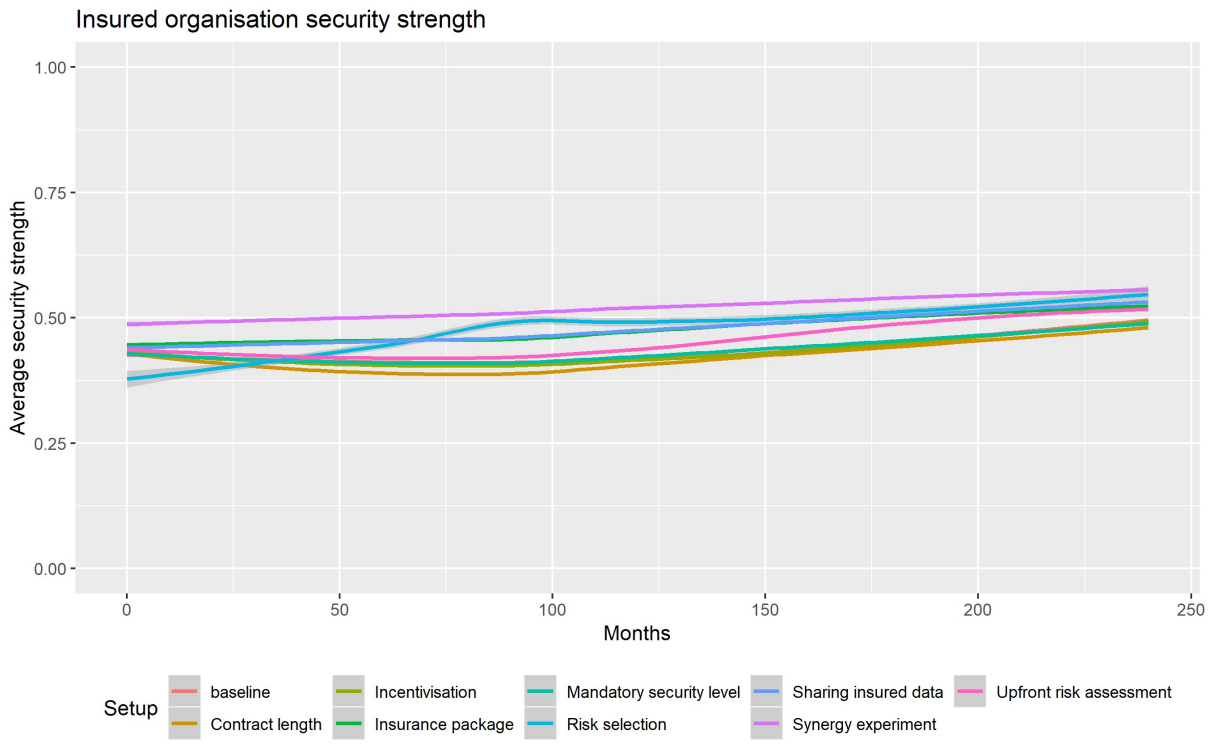

Figure 3: Experiment performance on security strength of insured organisations

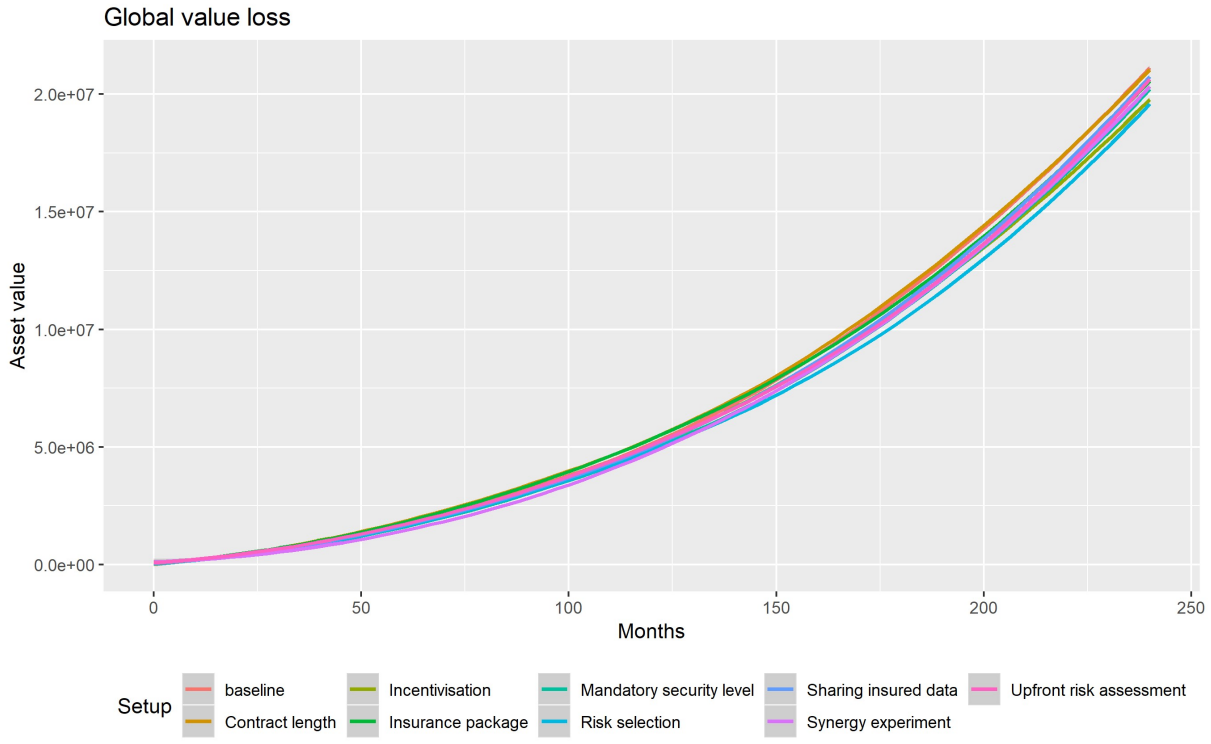

Figure 4: Experiment performance on the global value loss

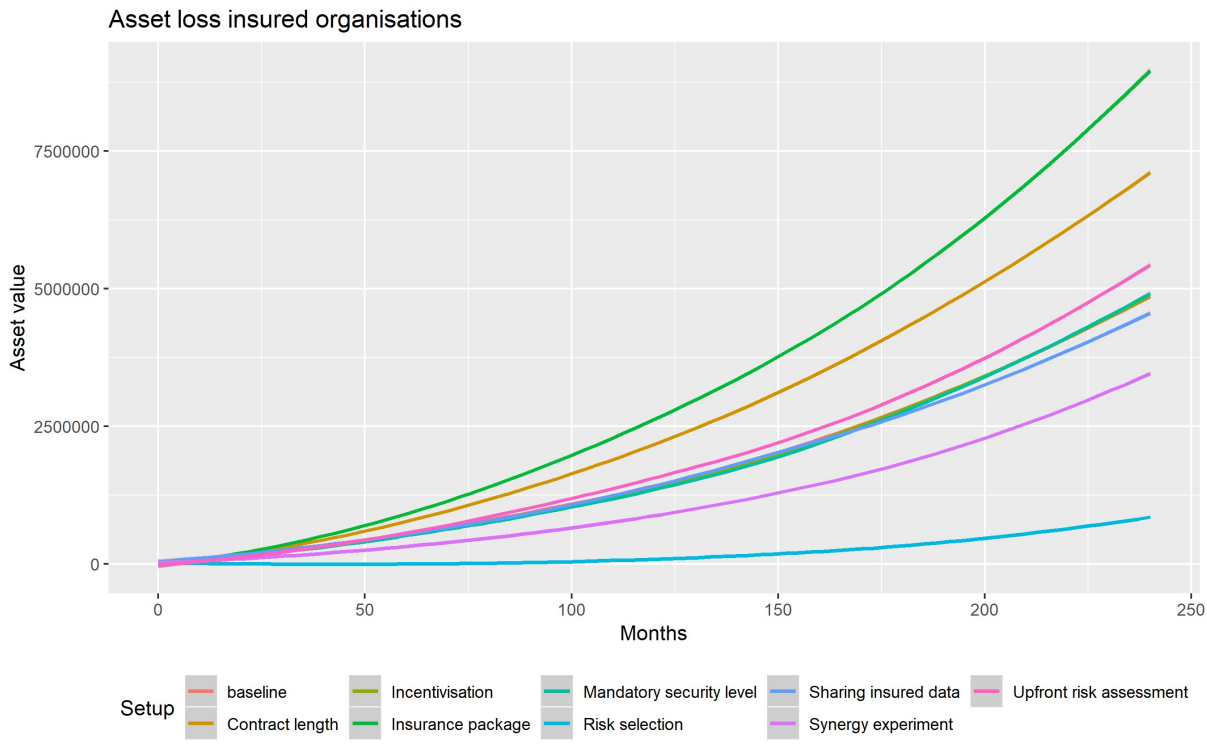

Figure 5: Experiment performance on asset loss of insured organisations

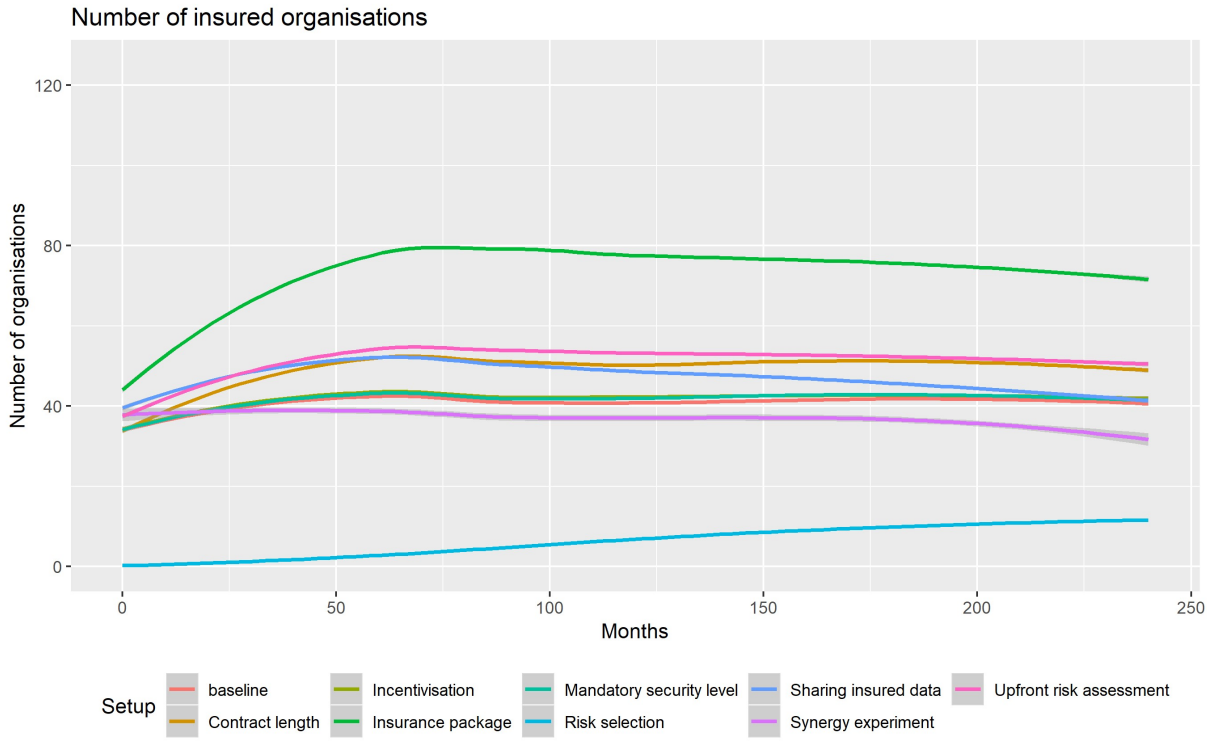

Figure 6: Experiment performance on the number of insured organisations

6. Conclusion and discussion

The research question posed in this study was: *How do various cyber insurance policies influence the cyber security ecosystem?* In order to answer this question an agent-based model was created which simulated the cyber security ecosystem. Furthermore, by researching insurance policies and the possible options to influence the ecosystem, seven policy options were identified. Through the use of the ABM model these policy options were experimented with and a synergy experiment was also created and tested. Unfortunately, the results showed very little differences making it difficult to state anything as very useful. However, whilst small and with some side-effects, nearly all policy options showed positive effects on the system. The synergy experiment also seems to provide the most beneficial performance compared to the other policy options. The small differences could be attributed to a number of things. However, the largest reason can be found in insurance in a general sense. Insurance is inherently bad for the ecosystem. This is because risk is displaced without increasing the cyber security level. Thus an insured organisation gets attacked / breached more often but doesn't actually feel the damage since its insured, meaning that the organisation can still have an improved welfare by using cyber insurance. The experiment also showed that the number of insured organisations played a large role in the small influences observed. This is because insurance policies can only exert influence on insured organisations, thus with fewer insured organisations the effects will become harder to notice.

The main limitations of this study lies in the unavailability of real data. Very little data can be found on the values that should be used for certain mechanisms. Furthermore, the data that is available is usually aggregated making it unusable as data input. Other limitations concerns the assumptions made to come to this model and the ecosystem level abstraction that was necessary. This has caused for complex mechanisms to not be modelled or be implemented in a simplified state. This can cause behaviour to become limited and can lead to different results which might not hold true in the actual system.

However, the ABM model that was built in this study provides great insight from a dynamic perspective. Furthermore, the effects of insurance policies have been tested and insight has been obtained on the influence of these policies. Furthermore, the model itself can be adjusted and improved in order to gain better or different insights.

Future research should also focus on utilising this and other dynamic models to study the influence of cyber insurance. This can increase the understanding and allows for exploration of the ecosystem to find better insurance policy options to influence the system.

References

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.

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.

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).

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

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

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).

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

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.

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).

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.

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

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

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. Simplifying assumptions

As mentioned in section 4, several simplifying assumptions have been made in order to reduce model complexity and keep the model workable. The simplifying assumptions are described below.

Organisations

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.

Attackers

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 gain if they are successful.

Insurance firms

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.

External environment

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.

Appendix B. Formalised model

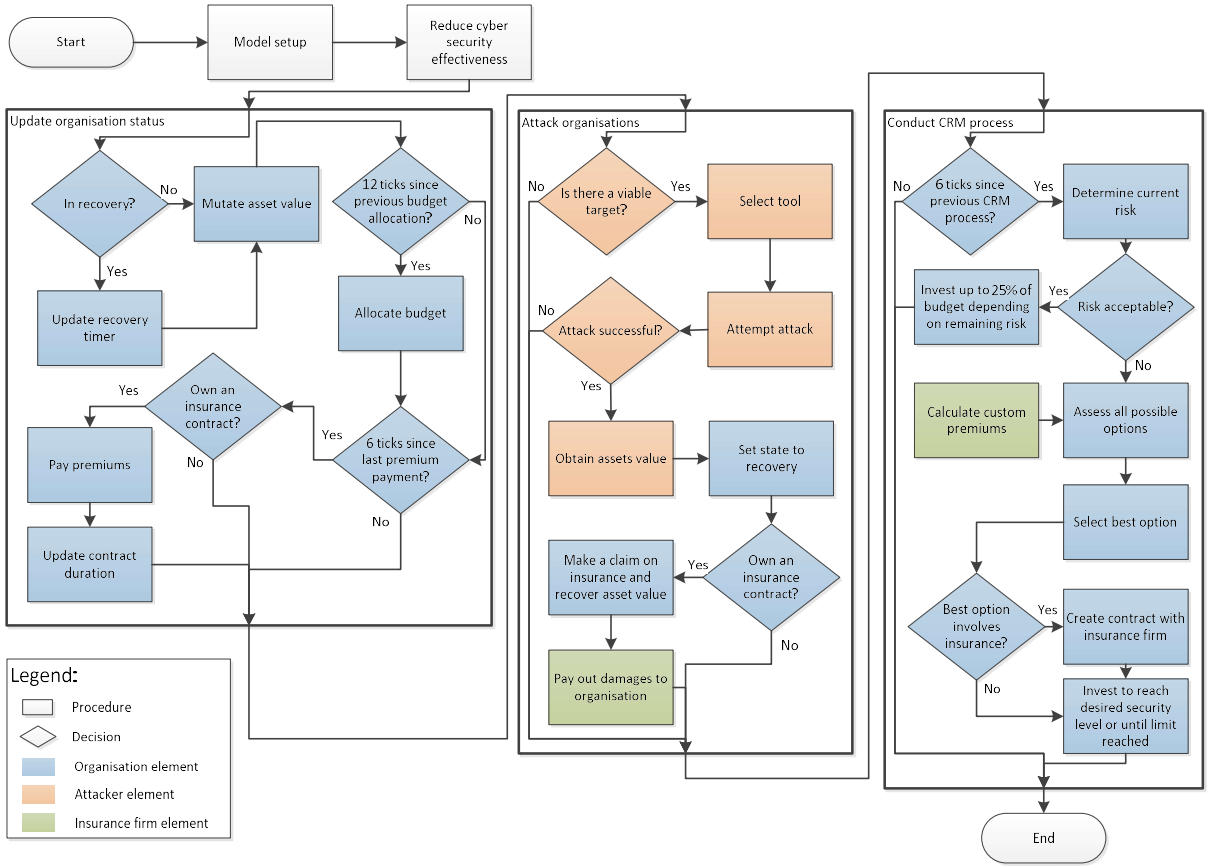

Figure 7: Overview of formalised model procedures