Abstract

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

This is the second paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

And after the second paragraph follows the third paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

After this fourth paragraph, we start a new paragraph sequence. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of

the original language. There is no need for special content, but the length of words should match the language.

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Preface

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1
Introduction to Cyber Insurance

Cyber-insurance is an insurance product used to transfer financial risk associated with computer and network related incidents over to a third party. Coverages provided by cyber-insurance policies may include property loss and theft, data damage, cyber-extortion, loss of income due to denial of service attacks or computer failures [PD12]. Traditional coverage policies rarely cover these incidents, therefore cyber-insurance is seen as a huge potential market. Although the concept of cyber-insurance has been around since the 1980s, it has failed to reach its promising potential. There might be several reasons for this slow development, however, it is believed that the main reason so far, is that no model deals with all the unique problems of cyber-insurance at once. In addition to the known difficulties of insurance, cyber-insurance has to deal with the problem of nodes asymmetric information, correlated risk and interdependent security [GGJ+10]. These three problem areas will be discussed in detail later in 1.3. First let's have a look at the similarities of normal insurances and cyber-insurance.

The basics principles of cyber-insurance relates to traditional insurance, where the insurance contract (policy) binds the insurance company to pay a specified amount to the insurance holder in case certain incidents occurs. In return, the insurance holder has to pay a fixed sum (premium) to the insurance company [Rob12]. As with other insurances, the cyber-insurance contract is signed between the insurance company and the insurer. The contract clearly specifies the type of coverage of the different risks, a risk assessment of the companies vulnerability and also an evaluation of the companies security systems. These assessments are used to calculate the companies premium [Rob12]. Generally, this means that the security is negatively correlated with the premium costs. Better security means lower price on the insurance premium.

1.1 The basics of insurability

Generally, from the perceptive of the insurance company an insurable risks possesses seven distinct characteristics [MCR80]:

1. Large number of similar exposure units: Insurance companies is based on the principle of pooling resources, where insurance policies are offered to individual members of a large class, meaning the more insurers the predicted losses is closer to the actual losses.
2. Definite loss: A loss should take place at a known time, in a known place and from a known cause. Incidents such as a fire or car crash, are examples where these terms are easy to verify.
3. Accidental loss: The event that triggers a claim should not be something the insurer has discretion or control over.
4. Large loss: The size of the loss must be meaningful from the perspective of the insured. Insurance premiums need to cover both the expected cost of the loss, in addition, cover all the expenses regarding issuing and administrating policies, adjusting losses and supplying the capital needed to be able to pay claims.
5. Affordable premium: The premium must be proportional to the security offered, otherwise no one will offer/buy the insurance. In the situation where the likelihood of the insured event is high, and the cost is large, it is unlikely that the insurance company will offer the insurance, or at least the premium would be too high for anyone to consider buying it.
6. Calculable loss: Both the probability and the cost of an insurable event, has to atleast be possible to estimate.
7. Limited risk of catastrophically large losses: If losses happen all at once the likelihood of the insurance company getting bankrupt is high. Therefore, losses are ideally independent and non-catastrophic.

1.2 The idea behind cyber-insurance

When facing risk, there are typically four options available:

1. Avoid the risk
2. Retain the risk
3. Self protect and mitigate the risk
4. Transfer the risk

So far the risk management for computer networks have introduced methods to reduce the risks, a mixture of option 2 and 3. This has lead to creation of systems

and software trying to detect threats and anomalies and to protect the users and the structure from these threats. Anti-virus software is also a good example of a system which perform self protection and hence mitigate the risk of becoming a victim of malicious attacks.

Unfortunately these types of systems does not eliminate the risk. Threats evolve over time, and there will always be accidents and security flaws. Cyber-insurance acts in the domain of the fourth option, and seeks to answer the question; -how can one handle this residual risk. The basic idea for cyber-insurance and insurance in general is to transfer the risk to a party who willingly accept it in exchange for a predictable periodical fee, namely premiums [BL08].

1.3 Three main obstacles

As we have seen, cyber-insurance fit relatively well to the general insurance model, however there are some identifiable obstacles. These obstacles can be divided in to three categories, information asymmetry, interdependent security and correlated risk.

Information asymmetry Information asymmetry arises when one side in a transaction or a decision has more or better information than the other party. There are two different cases of information asymmetry, the first one is called adverse selection, where one party simply has less information regarding the performance of the transaction. A good example is when buying health insurance, if a person with bad health purchases insurance, and the information about her health is not available to the insurer, we have a classical adverse selection scenario. A similar case for the security industry occur when buying insurance for your computer, and the insurance company has no way of confirming whether your computer is "healthy", i.e. not contaminated, or if it is infected. The other information asymmetry scenario is called moral hazard. It occurs when after the signing of the contract, one party deliberately takes some action that makes the possibility of loss higher, i.e. choosing not to lock your door, since you have insurance. Or in the computer setting, deliberately visiting hostile web-pages, or not using anti virus software, firewalls or other self-protection software. [Pal12]

As we will see the information asymmetry problem is highly relevant regarding cyber insurance. Measuring the level of security is very hard, in addition will often people have an incentive for hiding information about their security strength. Because they might end up in a scenario where they describes what their weaknesses are, and thus the difficulty of successfully attacking them are lowered. Another problem arising due to information asymmetry, is the so called lemons market [1]. It is difficult

[1] Lemon market, the problem of quality uncertainty, was first introduced in a paper [Ake97] by

for a security software buyer to distinguish the performance(bad vs good) of different software products, and thus the reasonable thing to do, is to buy the cheapest. From this we see that every security software has to be sold at approximately the same price, and there is no way to distinguish good and bad software. If the cost of producing good security software is to high, the problem can even result in abandoning the production of good software, because it would not be profitable.

Correlated risk Another big concern regarding cyber-insurance, is the correlated risk. Among others the problem occurs due to the need of standards. Standardization is an important part of computers and computer networks, it enables computers to communicate, install and use different software. A good example is the operative systems for personal computers, today we only have a small set of operative systems available for use, and these systems have been standardized, such that they can communicate over the same communication channels, such as HTTP/IP. The standards are what makes the ICT-industry valuable, but also what makes the possible extent of the threats so large. All these systems that uses the same standards, creates a large number of similar exposure units, they share common vulnerabilities, which can be exploited at the same time.

A different scenario is natural disasters, If the backbone network is down for numerous reasons, every operator connected will loose the Internet connection, hence be entitled to receive compensation for the lost income.

This creates a significant difficulty for the cyber-insurance industry, because when a security breach occurs there is a high probability that it will occur to a large number of people, i.e catastrophic and extreme events occurs more likely, resulting in extremely high expenses. If the security breach is large, it could potentially cause so much damage, that the insurers will not be able to pay all of the customers who suffered, i.e. they go bankrupt.[BS10]

Interdependent security Investment in security generates positive externalities, and as public goods, this encourages to free riding. Why should I pay for security when I can just free ride on security invested by others. The problem is that the reward for a user investing in self-protection depends on the security in the rest of the network, i.e. The expected loss due to a security breach at one node, is not only dependent on this nodes level of investment in security, but also on the security investment done by adjacent nodes, and theirs adjacent nodes and so forth. A good example of this is the amount of spam sent every day, which is dependent

the economist George Akerlof in 1970, and used the market for used cars as an example.[Wik] The conclusion of the paper is that since the buyers lack information to distinguish a bad car(lemon) from a good one(cherrie), the buyer will not pay the price the seller wants for a cherrie, and the seller will not sell a cherrie for the price of a lemon, and thus the lemons drives the cherries out of the market.

on the number of compromised computers. Meaning if you have invested in security software of some kind, you still receive lots of spam due to the fact that there are a variety of people who have not invested [Böh10].

1.3.1 Other obstacles

Calculating loss Another concern regarding cyber-insurance relates to characteristic of calculating loss from [MCR80]. When facing a security breach there are to potential loss classes:[BMR09]

- primary losses or first-degree losses: direct loss of information or data and operating loss. These arises from disuse, abuse or misuse of information. And the cost of these arise from recovering, loss of revenue, PR and information sharing costs, hiring of IT-specialists etc.
- Secondary losess are indirectly triggered. These are the loss of reputation, goodwill, consumer confidence, competitive strength, credit rating and customer churning.

The value of the loss from both these classes can be difficult to determine, although the second one is probably the most difficult. Because it is challenging to put a value on i.e. how many potential customers did they loose due to the reputation loss, how many customers churned, and what was their value etc.

Cyber-insurance instead of security One problem with cyber-insurance is actors seeing it as a solution to the problem of being secure. Instead of investing in security, they now have a way of buying their way out. However, this problem might solve it self with the right pricing options. Meaning that the insurance companies can create pricing models which makes it economical beneficial to invest in security. Such model will also make sense for the insurance company, since better security systems yields lower probability for incidents. Similar pricing models are common through out the insurance industry, e.g. the bonuses a car driver might be offered due to no accidents for some time or being above a certain age etc. will lower the price the insurance premium.

1.4 A small summary

Add a small summary here.. summary of related work

short presentation of what to come. "glidende overgang til current market".

Chapter 2
Current market

2.1 Current market state

Carriers in London, New York, Zurich, Bermuda, Europe, the U.S. and elsewhere developing cyber-security insurance products for their clients. In UK there are 9 insurers with specialists in cyber devisions, in the US it is 30-40. [Ris12] There are lots of challenges both for buyers and sellers. Buyers face tremendous confusion about cyber risks and their potential impacts on business. People dont know or understand what kinds of risk cyber inlcudes, how large losses can be and why should they care about externalities? [PpD12] Even when companies have decided to purchase a cyber insurance, they are confused of what kind of insurance they should purchase. The market of cyber insurance becomes a lemons market, where the buyer have little knowledge to choose between the different insurances. Therefore, people will buy the cheapest insurance, which probably won't cover the expenses when the incident occurs.

notes... A survey of the Norwegian insurance market relieved that only one out of the five biggest actors [1] where even considering to offer something similar to ciber-insurance. From mail correspondence with Gjensidige it was clear that normally this was a typical risk they would like to insure, however with enough information exceptions could be made. The requested information was related to a companies revenue from a website, and a model describing the architecture of the server and it's value. Email from: Arild Hjelde, Gjennsidige Nor. end notes...

Despite the widespread awareness of cyber crimes, cyber attacks occur frequently. The companies studied in [Ins11] experienced successfull attacks every week. A successfull cyber attack can result in serious financial consequences. And the longer it takes to resolve the attack, the more costly it get. This paper found that the median cost of cyber crime is $5.9 million per year, ranging from $1.5 million to

[1] Gjensidige, If Skadeforsikring, DNB, TRYG, Storebrand

$36.5 millon per company, which is an 56 percent increase from the last year. This was in the US market only. With these numbers in mind, cyber insurance should be a very attractive security investment. More and more insurance companies are offering cyber protection, but there are still many companies not utilizing them, in a survey of 13000 companies, only 46 percent said they had a cyber insurance. [Pra]

Another paper [Ris12] collected statistics about cyber attacks in the UK, and the results said it costs £27 billion a year, and it is one of UKs biggest emerging threats. They found similar results as in US, the number of security breaches continue to increase, and it is not only large companies like google and playstation that suffer from attacks, but also small businesses. Despite these numbers there where only 35 percent of the companies in the survey who had purchased cyber insurance.

A lot of companies are trusting their own IT-department to handle cyber risk, and do not think they need a cyber insurance, despite the increasing cyber threats. [Wat11]

When comparing the norwegian Cyber Insurance market up against the US and UK, it is little information available of its current state. We did a survey and contacted some insurance firms, it was not possible to get any estimates on how big the current Norwegian market is. There are few actors offering any kind of cyber insurance, and as expected those who do are not eager to share information about their customer base, size, big/small-firms etc. Despite today's low activity, the survey revealed that around year 2000 there was taken steps towards establishing a cyber-insurance market in Norway. There where several startup companies, Safensure AS [dig], that where dedicated to deliver cyber-insurance to the Norwegian and European market, and some of the big firms , like Gjensidie Nor. They started offering insurance against lost income due to malicious hacker attacks, denial of service and other well know cyber-attacks. In 2001 Gjensidige Nor in cooperation with the German company Tela Versicherung offered businesses insurance against financial losses due to hacker attacks and sabotage for up to 5 million NOK, given that specified security measures were taken by the company [it]. Today, the same company offers something they call operation-loss-insurance which covers expenses due to denial of service, software-insurance which covers expenses regarding reconstruction of files and reinstalling software, it is also possible to insure against hacking and sabotage [Nor]. Unfortunately details specifying what's insured and the cost is not known. However, a similar insurance is offered by RTM Insurance Brokers, a Danish company, below is the offered premiums. This gives an indication of the cost of cyber-insurance in the Norwegian market. [Bro]

There are several different opinions regarding the health of the global cyber-insurance market. An article from CFC underwriting [New], a UK firm offering

insurance to small and medium sized business, claims promising numbers for the US cyber-insurance market. On US soil, 20-50% of businesses purchases either stand alone cyber-insurance or benefits from coverage provided in their already exciting insurance. Despite recent years focus on increasing cybercrime and the catastrophic consequences of weak security, Its only 1% of European businesses that are enrolled in an insurance program covering cyber-risks. One possible reason could be the different environments of the US and European market. In the US, 46 states have mandatory breach notification laws, combined with significant penalties for companies failing to protect sensitive data. This means that the US government are creating incentives for firms to buy cyber-insurance. In Europe, only Germany and Austria have similar breach notification laws, forcing companies to notify affected customers of data leakage. A recent proposal of the EU wants to introduce the notification law in Europe, and also include penalties for serious data breaches, these could be as high as 2 % of a companies global revenue [New]. It is proposed that the law should take effect in 2014, although this is highly unlikely regarding the complexity of the effects of this law. Undoubtedly this law would be a health injection to the rise of the cyber-insurance, however, a market based on fear of the consequences of not being insured is not beneficial. The ultimate goal for cyber-insurance, is to correlate the purchase of cyber-insurance with companies growing desire to invest in more security. The article claims that to meet this goal, the focus should be on the serious brand damage and not just the current financial loss. [New]

When facing a security breach there are two potential loss classes: primary losses or first-degree loss: direct loss of information or data and operating loss. These arises from unuse, disuse, abuse and misuse of information. And the cost of these arise from revovering, loss of revenue, PR and information sharing, hiring of IT-specialists etc. Secondary loss is indirectly triggered. Such ass loss of reputation, goodwill, consumer confidence, competitive strength, credit rating and customr churn. These claims arise from loss of external parties, sensitive data, and generally contribute to an even higher cost. [BMR09]

These two loss classes can be covered by cyber-insurance, usually are these contract based on the same two classes, i.e you have to get an insurance for both. Here is an example contract from [CoA].

2.2 Contract structure

Travelers cyber insurance:

- Liability insurance.
    1. Network and Information Security Liability

2. communications and Media Liability
3. Regulatory Defense Expenses

– First party insuring agreements:

1. Crisis managment event expenses
2. Security breach remediation and notification expenses
3. computer program and electronic data restoration expenses
4. computer fraud
5. fund transfer fraud
6. e-commerce extortion
7. business interruption and additional expenses

2.3 Economics

Traditional security is a public good and are usually provided by the government. The threats are also originating from a small number of actors. What about internet security, should it be handled by the government. We do not have anti-tank gear in every house, should we have anti virus software on every computer? there are strong externalities involved, if a unsecured computer joins the internet, it end up dumping costs on others, just like pollution. Lemons problem, antivirus software. because the customer cant see the difference. Asymmetric information explains many market failures, low prices in lemons-markets, why sick people struggle with getting to buy insurance. A good example of misaligned incentives is bank frauds in US and UK, in US the banks are the ones hold responsible, in UK it is the customers. One would think the banks in UK was better off, but they are not. Similar problems can be found in other systems, and the problem is security failing because the people guarding a system are not the poeple suffering the costs of failure.

2.4 Epidemics

[EK12] The social network within a population, has a big say in determining how diseases is likely to spread. it can only spread if there are contact between to persons(Nodes), the contact network. The contact network for to different diseases can differ radically, e.g java viruses versus worm propagating through another vulnerability. Or internet viruses versus viruses that spread through short-range wireless communication.

2.4.1 modeling contagion

branching processes first wave, a person carrying a new disease enters a network, and transmits to everyone he meets with a probability of p, he meets k-people. second wave, each person from the first wave now meets k new people, i.e a total of k times k and if infected passes the disease on with probability p. further waves are formed in the same way. With this simple modeling approach, we get a tree, with a root node which creates branches to new lvls of the tree. With low contagion probability, the infection is likely to die out quickly. If the disease in a branching process ever reaches a wave where it fails to infect anyone, then it has died out. It is only two possibilities for the disease in a branching model, either it dies out, or it continue to infect infinitely many waves. These two possibilities can be differentiaded by a quantity called the basic reproductive number. R_0, this is the expected number of new cases of the disease caused by one person/node. In this basic model this number is: $p * k$. If $R_0 < 1$ then with probability 1 the disease dies out after a finite number of waves, if $R_0 > 1$ then it continues to infect atleast one person each wave with a probability greater than 0. A interesting thing to notice about these statements, is if the R_0 is close to 1 in either way, then a small shift in the probability will change the disease status from terminating to widespread or visa versa. This suggests that around the critical value $R_0 = 1$ it can be worht investing large amounts of effort to produce small shifts in R.

SIR epidemic model Can be applied to any network structure, preserve the basics of the branching process at the level of individual nodes, but generalize the contact structure. A node goes through three potential stages:

1. Susceptible(S): Before the node has caught the disease.
2. Infectious(I): once the node has caught the disease, it is infectious and can infect other susceptible neighbors with probability p.
3. Removed(R): After a node has experienced the full infetious period, it is removed from consideration, since it no longer poses a threat.

Network with directed edges. The progress of the epidemic is ontrolled by the contact network structure, probability of contagion and t_I the length of infection. When a node enters the I state, it remains infectious for a fixed number of steps t_I. During each of these steps it has a probability of infecting its neighbours. After t_I it is removed(R). Good model for disease you can only catch once in a lifetime. Important to note that in networks that do not have tree structure, the claim made earlier about $1 > R_0 > 1$ does not necesarily hold anymore. The network structure is very important, it can decide if a disease will spread or not. Narrow channel example.

Extension to SIR The SIR model is simple, to make it more realistic we can add probability q of recovery, and also add different probabilities for contamination between nodes, due to stronger contact. We add periods to the infection time, early, middle and late and allow different probabilities for infecting in each of these states.

Model from dynamic to static(Percolation) assing a probability of infecting on every edge, calculate this at the beginning, and thus an infected node has to connected to another infected node by an open edge. Think of it as fluid running through open and closed pipes. Its only the open ones who can be affected.

SIS epidemic model Nodes can be reinfected. Only two states, susceptible and infectious. Researchers have proved "knife-edge" results on these networks as well. A SIS epidemic can be represented by a SIR model by using a "time-expanded" network. Duplicate the nodes to the next time-frame.

SIRS Epidemic model Remain removed(immune for a fixed period of time) t_R, this model fits good with many real world diseases. It can produce oscillations in very localized parts of the network, with patches of immunity following large numbers of infections in small areas.

2.5 Incentives and Information Security

People have realized that security failure is not only caused by technical mistakes but also misaligned incentives. When the person guarding them is not the one who suffers when the system fail, there are strong misaligned incentives. As the book [And10] states, the tools and concepts of game theory and microeconomic theory are becoming just as important as the mathematics of cryptography.

Informational asymmetries peer-to-peer network, these exploit network externalities to the fullest by having large member populations with a flat topology. Joining creates the possibility of collaboration with everyone. it is easy to cheat.One solution, change the network topology, create clubs of nodes, one need to establish trust with the club, then you can connect with outside groups through your group. Social networks can also be used to create better topologies, when honest players can select their friends as neghbors., they minimize the information asymmetry present during neighbor interactions. Another information asymmetry in security, is due to our inability to measure software security. Network science and information security, the network topology can strongly influence conflict dynamics. Externalities makes security problems reminiscent of environmental pollution, public goods.

Chapter 3
Graph Theory

In nature and human societies there are lots of scenarios that can be described by using graphs and graph theory, from infrastructure, such as railroads, water pipelines and electricity grid, to societal relationships, disease epidemics and much more. Additionally computer networks, such as peer-to-peer networks, number of links to/from web-sites etc, is formed and evolves according to the laws of random graphs. When one can describe a phenomenon with graphs, it is much easier to analyze and find characteristics about the phenomenon, the graph serves as an analytical tool [Aud]. Our goal is to identify insurable graphs, such as graphs which yields higher security or graphs where the risk is calculable. This section will provide background information on how different graphs can be created and how they evolve.

There are some basic properties of graphs which is important to be familiar with. Figure 3.1 depicts the basics of an unweighted graph, the edges are not assigned any value. Weighted edges can be useful to e.g. reflect capacity constraints such as a link's maximum bandwidth, or the length of a road(edge). Other common definition used when describing graphs are listed below [Aud]:

- Edge degree: Number of edges connected with a node.
- Hub: Node with high edge degree.
- Cycle: A chain originating and terminating at the same node.
- Cluster: Subgraph of highly connected nodes.
- Cluster coefficient: Probability that two nodes that are adjacent to a third node are also adjacent.
- Clique: Subgraph where all nodes are adjacent (cluster coefficient = 1).
- Small world graph: Graph with small diameter and large cluster coefficient (e.g. the Internet and A-B graphs, described in section 3.1).

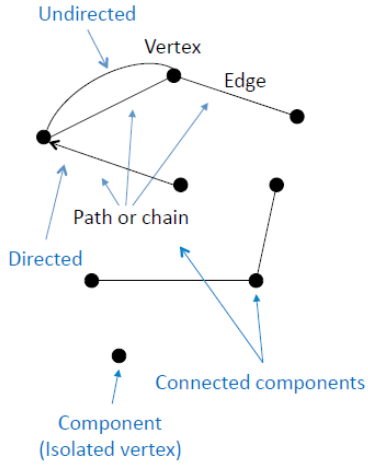


Figure 3.1: General graph [Aud].

3.1 Random Graphs

Cyber-insurance cover many fields, from financial transactions and outsourcing of tasks to computer networks, many of these fields share a common characteristic, they can all be described as a graph, and often a random graph. Therefore the study of random graphs are of special concern. The research on random graphs are fairly new compared to other mathematical discoveries. E-R graphs were first studied in 1959 by Erdös and Rényi, later and probably with more promising results was the graphs studied by Albert-Barabási in 1999 [Aud].

Erdös-Rényi Graphs E-R graphs is a network created between a fixed number of n-nodes, where each node connects to another of the $n-1$ nodes with probability p. The resulting graph will on average contain $n(n-1)p/2 \approx n^2p/2$ edges [Bol85]. By analysing the graph, the authors found some interesting properties:

- If $p < n^{-2}$ then there is no edges in the graph.
- If $p = c/n$ where c is a constant between $1 < c < log\, n$, the graph will provoke a single large component to grow within the graph.
- If $p > (ln\, n)/n$ then the graph is completely connected.
- If $p = 1/n$ triangles start forming in the graph.

A fully connected E-R graph will have a short diameter similar to the Internet, and thus could be a very good desrcription of the internet. However, the edge degree follows a Poisson distribution, which means that the edge degrees are peaking around the average value [Aud]. Consequently E-R graphs does not capture the immense clustering coefficient which is present in networks such as the Internet. In other words, E-R graphs are not small world graphs, and another graph structure is needed to model computer networks. A interesting fact about these graphs are their vulnerability, these graphs are very vulnerable against random attacks, such as nature disasters, but robust against directed attacks. Due to the fact that if you remove all edges from one node, it does little damage, since the network is not dependent on single nodes, every node has approximately the same node degree, and it is the sum of all the nodes connections that creates the network.

Albert-Barabási Graphs The structure which is believed to be most accurate regarding modeling computer networks are A-B graphs. A-B graphs are different from E-R graphs since they are scale-free, meaning that the vertices does not have an constant value throughout the entire graph. The formation of an A-B graph results in multiple hubs with a high edge degree. Albert and Barabási found that the edge degree of each vertex follows a power law distribution; meaning that the probability that the edge degree is g is proportional to g^{γ} where γ usually is a number between 2 and 3 [Aud]. Consequently there are relatively high probability that there exists some nodes that have a very high edge degree. These graphs are in contrast to E-R-graphs, very vulnerable to directed attacks, because if you take out a hub, you suddenly destroyed the whole graph. But the graph is very robust against random attacks, this is why most of the networks we observe in the nature can be depicted as A-B-graphs. A-B graphs can grow and become scale-free if every new vertex is connected to one or more already existing node with a probability proportional to the edge degree of that node . The paper presents an algorithm that creates A-B graphs and figure 3.2 shows one graph that evolved from this algorithm:

- A new single vertex is added to the graph.
- This vertex is connected to exactly two other vertices in the graph.
- The probability that the new vertex connects to another vertex is dependent on the edge degree of the other vertex, higher edge degree meaning higher probability
- There is only one edge between two vertices.

In addition to the high clustering coefficient they showed that A-B-graphs have a fairly small diameter, which can be seen in figure 3.2. A-B graphs are therefore comparable to the network formation of the Internet and other computer networks.

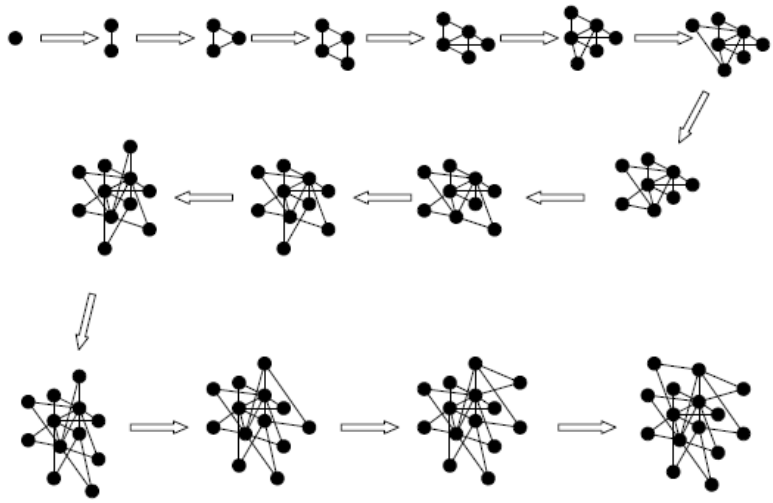


Figure 3.2: Forming a A-B graph in 15 generations [Aud].

3.2 Real world graph structures

The internet, the World Wide Web, neural networks, scientific referencing and co-authorship, stock markets, airline routes, food webs, and modular software systems, all tend to evolve in a way similar to that described in the examples above. This section will provide some real world examples of how complex systems with huge amount of data can be described as network structures having the same characteristics as A-B graphs.

Stock markets The research paper: [Gar07], analyzes the correlation between different stocks in the Greek stock market in year 1997. They compared the daily closing price of stock i at day t, and compared the similarity of a pair of stocks i and j by using the correlation coefficient. The idea is that the correlation coefficient between a pair of stocks can be expressed using different distances in a graph structure. A short distance means high correlation and long distance means low correlations between the stocks. Normally this network would be shown as a fully connected graph, which will consist of $\frac{n(n-1)}{2}$ edges, and would be difficult to analyze. However the approach taken in the paper will present a clear understandable graph consisting of $(n-1)$ edges.

The resulting graph can be seen in figure 3.3, and show a network consisting of several clusters linked together. Instead of having to analyze a complex system with huge amount of data, this stock market can be analyzed by its topological properties,

such as the high clustering coefficient, i.e a star-topology, which will among others point out which stocks have the most influence on others.

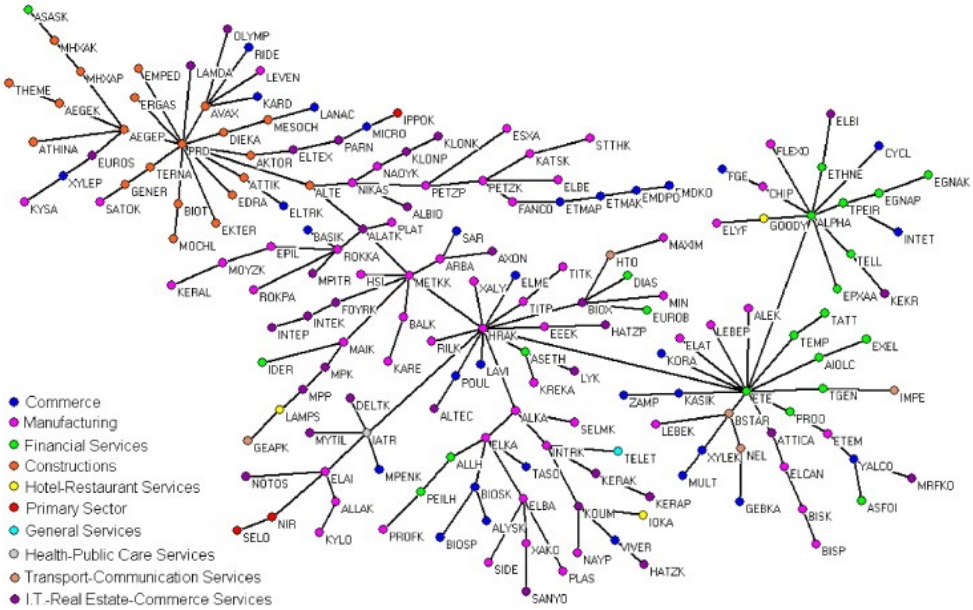


Figure 3.3: Network obtained by comparing two stocks correlation coefficient in the Greek stock market (Athens Stock Exchange, ASE) in year 1997. The different colors represent the different sectors of economic activity [Gar07].

Airline routes Another real world network which shows the same characteristics as scale-free graphs is the map of airline routes. Figure 3.4 shows the US route map of the American airline company, SkyWest. The characteristic clustering emerges in the figure, where a majority of the flights departs from either Denver, Chicago or San Francisco. Not surprisingly, these airports are all in the top 7 busiest airports in the US [Faa], and serves as hubs for many of SkyWest flights. In the airline industry some airports are called hubs, because that's what they are, - a connection point for major parts of the network of flights. The network of flights, as depicted 3.4 follows the characteristics for A-B graphs. From the graph, we see that the network are vulnerable against direct attacks, meaning if an low edge degree airport is shut down, there will be little consequence for the rest of the network. However, if one of the hubs is forced to close, it will provoke huge delays through out the whole network of flights, because many of the destinations are interconnected via the hubs.

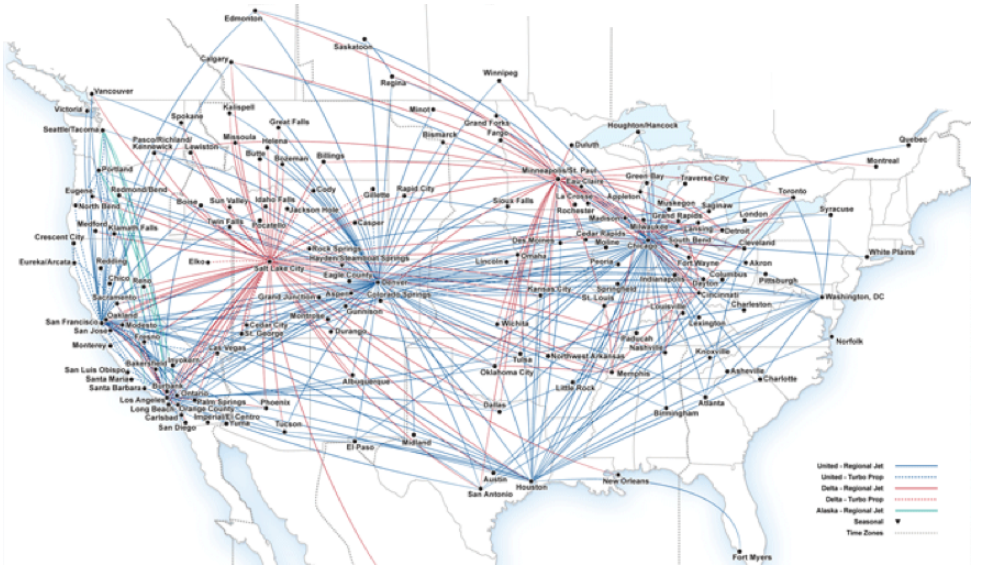


Figure 3.4: SkyWest Airline combined route map [CfAPA].

Similar findings will appear in the different networks mentioned earlier in this chapter, and all of them will experience large consequences if a hub in the network stop functioning. This is important for cyber-insurance because the many of the networks we are analyzing tends to look and behave like A-B graphs. For example, transactions between companies, big companies probably have more transactions than small companies, and thus creates a hub, this can be compared with how the correlation between stocks in a stock market works. I.e. we can say that small firms correlate highly with big-firms. NOTES!!! Geek stockmarket graph: http://www.sciencedirect.com/science/article/pii/S037843710700221X

Hvorfor er slike strukturer viktige å forstå for oss? Som vi skal se senere oppfører hubene seg i A-B grafene som stjerne-topologier. Ved å ha oversikt over sitt eget nettverk vil man kunne identifisere hvor disse stjernene befinner seg, nettopp disse er det viktig at man sikrer for å ungå spredning av virus, samt fungere som en blokkade mot andre trusler e.g. hackers. (TROR DET er viktig at vi prøver å fokusere mot insurable og ikke spredning av virus.) så noe sånt: nettopp disse er viktige slik at man lettere kan kalkulere riskioen, og gi insentiver, ved hjelp av cyber insurance, til hubsa for å sikre seg eller no.

Chapter 4
Evolutionary dynamics on graphs

When investigating cyber insurance and insurable topologies, it is important not to only focus on standard risk networks, such as the internet. Our goal is to investigate all kinds of networks, or especially networks where players actions are influenced by their neighbourhood structure, i.e. the network connections will affect each individual players payoff. In this case there are several types of networks to consider, all social and economic interactions where an agents well being is dependent on externalities as well as her own actions, is a network worth considering network.

As mentioned earlier, the internet is a very good example, because on the internet we are "all" connected, the benefit we get from the internet is strongly dependent on this, and so is the risk we face when using the internet. Other examples could be the networks that are formed when a company are developing a software product, this development process is often done by several different firms, and thus creates a development network, where everyone is dependent on the result of the others. If one or more fail in some way, bankruptcy, failure to deliver at the expected time, higher cost etc. Then the whole network will be affected. Or in a cloud computing network, there are many different users and internet service providers, and the overall security is dependent on all of them. As we see all these networks are different from each other, some face direct connections, other consist of social and economical connections. But they all share some main characteristics, they are all experiencing network effects, externalities, information asymmetry, correlated risk and interdependent security. [GGJ+10]

In our paper an insurable topology, is an network structure which makes it feasible for both the insurer(supply side) to offer and the customer(demand side) to acquire insurance. For this to be possible there are many difficulties to overcome, one example are the correlated risks, from the insurers point of view, the problem is to be able to calculate the overall probability of casualty/infection, which can be very difficult without graph theory.

The paper [LHN05] is about evolutionary dynamics and how certain structures can amplify or sustain evolution or drift[1]. To be able to find insurable topologies, an extensive study of different graphs and how they behave has to be conducted. Regarding security, knowledge of how viruses spread and how to use graph structures to prevent malicious hackers from entering your network is important. Evolutionary dynamics, and the research of how mutant genes spread though out a population is a very useful field when looking for an insurable topology. If one can determine some structures, where some nodes are advantageous/disadvantageous , then these structures will have certain properties, such as sustaining viruses from spreading, or amplify the incentive for obtaining cyber-insurance and protection software. If one could identify these nodes and networks, then this information could be used to determine if it is an insurable topology.

In the [LHN05] paper, they show that mutants inserted in to a circulation graph, will have a fixation probability equal to

$$p_1 = \frac{(1 - \frac{1}{r})}{(1 - \frac{1}{r^N})} \tag{4.1}$$

Where r represents the relative fitness of the mutant, if it is advantageous it will have a certain chance of fixation, and disadvantageous mutants will have a chance of extinction. A circulation graph is a graph that satisfy these two properties:

1. the sum of all edges leaving a vertex is equal for all vertexes
2. the sum of all edges entering a vertex i equal for all vertexes

The fixation probability determines how probable it is that the whole network will eventually be "infected" by the mutant. I.e. it determines the rate of evolution, which relies on both the size of the network and the evolution speed. A probability equal to one means that every node in the network eventually will be affected by the mutant. A circulation graph is not necessarily an insurable topology, but if we can find graphs with fixation probability that exceeds equation 4.1 they could possibly be considered as insurable topologies, because if we can find these graphs, then it will be possible to suppress drift and amplify selection and visa versa. The paper shows that there exists such graphs, one example is the star topology. (see figure 4.1) In this topology the fixation probability is as shown in equation4.2, or for more general see equation 4.3

$$p_2 = \frac{(1 - \frac{1}{r^2})}{(1 - \frac{1}{r^{2N}})} \tag{4.2}$$

[1]Drift is the opposite of selective evolution , it is when the network/structure evolve and change at random

. or more generall:

$$p_k = \frac{(1 - \frac{1}{r^k})}{(1 - \frac{1}{r^{kN}})} \tag{4.3}$$

When comparing the equations 4.1 and 4.2, we see that the selective difference is amplified from r to r^2, i.e. a star act as an evolutionary amplifier, favouring advantageous mutants and inhibiting disadvantageous mutants.

There exists other graphs where the fixation probability is equal to 4.3, examples are super-stars, such as funnels and metafunnels. These are just more complex star networks. This paper shows, that the super-stars if N is large enough, the fixation probability for an advantageous mutant converges to 1, and for disadvantageous converges to 0. As we know from chapter 3, there are many topologies in our society that are so called scale-free. Scale-free networks have most of their connectivity clustered in a few verices, the star and the super-stars are all scale-free, and scale-free networks are potent selection amplifiers.

Star-network as an insurable topology The paper [GGJ+10] shows how network games evolve when the payoffs are determined not only by your own decisions, but also by your neighbours. This can be used to analyze the insurable-topology, star network, further. One of the games they analyzes is simple but highly relevant for our paper, a public goods game. A good example of a public goods is security product, because it suffers from strategic substitutes, i.e. if your neighbour acquire the security product, you have less incentive of also acquiring the security product,

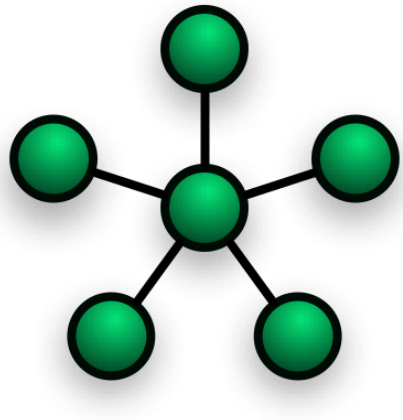
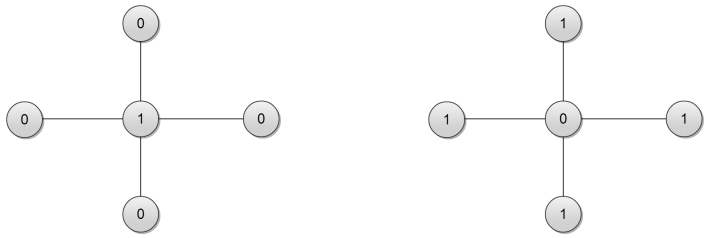


Figure 4.1: A star-topology [LHN05] .

because when he acquire it, he gets more secure, but so do you, due to the positive externalities of the product.

Lets consider a simple game shown in this paper, We have an action space: $X = \{0, 1\}$, where 1 can be considered as acquiring information, take vaccine, buy security software etc. And 0 is not doing so. Each node i has a set of neighbours: N_i, and a payoff function $y_i = x_i + \bar{x}N_i$. The gross payoff to player i is 1 if $y_i >= 1$ and 0 otherwise. But each player also suffer from a cost of $0 < c < 1$ if they choose action 1. When looking at 4.2, we easily see that there is two equilibriums. One



(a) Socially Optimal equilibrium, center node choose action 1

(b) Non Socially Optimal equilibrium, leaf nodes choose action 1

Figure 4.2: Figure 4.2a shows the socially optimal equilibrium, and 4.2b shows the non optimal equilibrium.

where the center node choose action 1 and the rest of the nodes choose action 0, and a second equilibrium where all the leaf nodes chooses 1 and the center choose 0. The overall payoff in these two differ from each other, the latter is not socially optimal because it suffers from a cost equal to: $\#leafnodes * c$, the first equilibrium have a total cost of only c. It would have been very good if we where able to force the game to end up in the social optimal equilibrium.

From a insurers point of view If a insurance company could identify these star-structures, and force them to end up in the social optimal equilibrium it would have been very beneficial for both the insurer and the customers. First of all if the insurer could identify these structures, he could calculate the overall probability of fixation by a diseased mutant(virus, worm, trojan or other failures) as shown earlier. And if they could ensure that the center node is protected they could also calculate the probability of the diseased mutant being extinguished from the network. One possibility of achieving this could be by offering very cheap insurance to the leaf nodes, and giving the center node an incentive to acquire security product, by informing the center node about the probability of failure unless he acquires security. And offer him a very good rebate if acquire the security product, and a very expensive

insurance if not. In this way the insurer could force a rational center node to getting both insurance and security product, and thus securing the whole network.

This is a simple scenario, analyzing an exogenous network formation [2], but it shows how a insurer can, by using the results from [LHN05], force the game to end up in the social optimal equilibrium, and also how the insurer can calculate the probabilities of failure. The contributes significantly to solving some of the problems with cyber-insurance. The problems with information asymmetry and interdependent risk problem has been reduced, since if the insurer knows the network structure, he can calculate the probabilities of failures and catastrophic events, the most important information he needs is how secure the center node is. If he also can ensure that the center node is secure, the interdependent risk problem is limited to only one node, the center node. All this result in a simple but insurable network topology.

4.1 Notater og slikt

4.2 NOTES... random.. don't read

The game: The way this game works, is that we look at nodes that are mutated (A), and those who are not (B).

When we apply the game to a directed graph, there are four different outcomes, a,b,c and d, which represents the interaction between the nodes, as is depicted in the figure below4.3.

In the first figure (Positive symmetric) the fixation probability is related to r=b/c. If b is greater than c, the properties of mutant b will propagate in to all the other nodes, and the whole graph will eventually consists of only mutated nodes. The opposite will happen in the case where c is greater than b, leading to extinction of the mutation. The later scenario models the situation where proper protection against a mutant i.e. a security threat is installed. If the level of security, c is higher that the strength of the security threat it will be blocked from propagating further into the network.

More generalized, W does not need to be stochastic, $w_{ij} >= 0$. If the sum of all edges leaving a vertex is equal for all vertexes, then the graph will never suppress selection. If the sum of all edges entering a vertex is equal for all vertexes, the graph never suppress drift. If both then the graph is called a circulation.

Where the fixation probability determines the rate of evolution, which relies both on the size of the network and the evolution speed. A probability of 1 means that

[2] Exogenous: The network formation is given. Endogenous: The structure originates from within the network, i.e. the oposite of exogenous

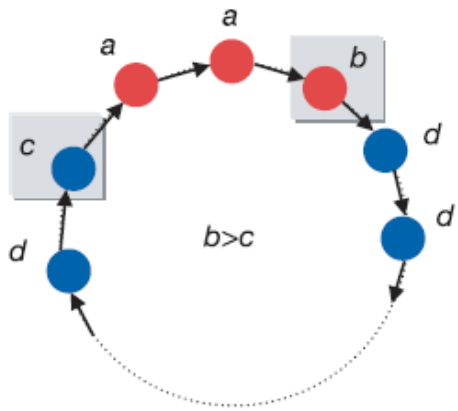


Figure 4.3: Mutant propagation game

every node in the network eventually will be affected by the mutant. Isotherm graphs are a sub-graph of circulation.

If W is symmetric, or isotherm then the fixation probability is always 4.1 isotherm means doubly stochastic, all rows and cols sum to 1. If a graph is one rooted, it has a fixation prob of $1/N$ regardless of r. If a graph has more then one root, its fixation probability is zero. Is it possible to find graphs with fixation probability that exceeds 4.1? Is it possible to suppress drift and amplify selection?

Chapter 5
Modeling Cyber-Insurance

5.1 Network Formation Games

In many scenarios agents seeks to create networks in order to directly benefit from each other. The established links might represent companies out sourcing part of their manufacturing, or cooperative agreements in the development of new software products. In addition to increase the trade-off, each of the established links represents risk of being a victim of cascading failures. The intuitive example is the spread of epidemic diseases, also node failures of a power grid and financial contagion such as the one back in 2008 was a result of cascading failures. Strategic network formation using cyber-insurance can be used to prevent such situation in addition to increase the overall payoff of participants in a clustered network.

When deciding whether to establish connection to a neighbor agent, the payoff has to be higher in the balance between the expected earnings and the risk of the other party failing to complete the transaction. This is the reason why we seek to only download content from trusted peers and outlaw MC-gangs are consistently skeptical to enter into new agreements despite promising increased earnings, since the risk of undercover police are too high.

The paper [Blu11] come up with some interesting results regarding network formation games. They set up a game where the nodes benefit from direct links, but these links also expose them for risk. Each node gains a payoff of a per link it establishes, but it can establish a maximum of δ links. A failure occur at a node with probability q, and propagates on a link with probability p. If a nodes fail, it will receive a negative payoff of b, no matter how many links it has established.

The results from their model shows a situation where clustered graphs achieve a higher payoff when connected to trusted agents, compared to when connecting with random nodes. Unlike in anonymous graphs, where nodes connect to each other at random, nodes in these graphs share some information with their neighbours, which

is used when deciding whether to form a link or not. To further explain these results, they show that there exists a critical point, called *phase transition*, which occurs when nodes have a node degree of $frac1p$. At this point a node gets a payoff of $fracap$, and to further increase the payoff the node needs to go into a region with significantly higher failure probability. Because once each node establish more than $frac1p$ links, the contagious edges, will with high probability form a large cluster. Which results in a rise in probability of node failure, and reduces the overall welfare. From this the paper say that when the minimum welfare exceeds $(1 + f(\delta) * fracap)$ we have reached super critical payoff. Otherwise it is called sub-critical payoff. Further they show that the only possible way of ending up with supercritical payoff, is by forming clustered networks consisting of cliques with slightly more than $frac1p$ nodes. If the nodes form an anonymous market, random linking, they can only get sub-critical payoff. In other words, if the nodes can choose who they connect with, and by doing so, creating trusted clustered markets, they can achieve a higher payoff, by exceeding the critical node degree point. But in random graphs, this is not possible.

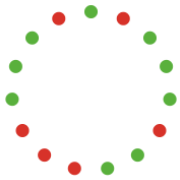
Inspired by this model, we are step wise building a model which shields light on how cyber-insurance can be used in network formation to prevent cascading failures and increase an agents payoff.

5.2 Model 1 - Initial Model

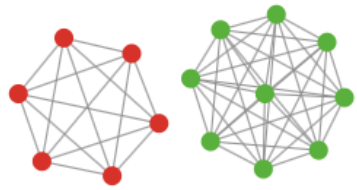
As a starting point the model is highly simplified in order to show the concept of how cyber-insurance can be used to create an insurable topology. Through out this chapter new features will be added to the model to make it more realistic and applicable. To begin, the model is formulated as follows. A set of n agents are randomly chosen to be insured or not, as depicted in figure 5.1a. They all get their own fixed income, and by connecting to other agents they will receive a benefit resulting in higher payoff. Non-insured agents will have a risk of failure i.e. an expected cost of failure. Therefore if an insured agents chooses to connect to a non-insured agent they will also suffer from this expected cost of failure. To simplify the decision process, the model follows a rule that only allows insured to connect to other insured agents and non-insured agents can only connect with each other. In addition we apply the assumption that each node goes through the whole graph to decide whether to establish a connection or not. Since the decision is bidirectional, meaning each agent must agree to establish the connection, the resulting graph will always be two fully connected cliques, one consisting of insured agents and the other of non-insured agents, as shown in figure 5.1b.

This dichotomy represents a trusted environment for the insured nodes, because they know that each node in the clique is insured against risk such as, financial catastrophe. These agents will benefit from each connection without having to worry

about contagious risks from the connected agents. An agent in the non-insured clique will also receive the aggregated benefits from the connections, however each of the connection has a probability of failure. Hence this environment is not trusted, and a decision on whether to connect will always involve some risk.



(a) 15 Agents randomly choosen to be either insured (green) or non-insured (red).



(b) Two clustered networks. One consisting of insured agents the other consists of non-insured.

Figure 5.1: Shows how agents connects to eachother according to model described in section 5.2.

There are many examples of nodes needing to establish connections, one example is a company needing to out-source certain tasks to remain competitive. This outsourcing involves some risks, such as, will the company deliver at the reported time, to the reported costs, what happens if they fail to deliver, what if they go bankrupt etc. If the companies that are going to establish links(cooperative contracts), know that the other firms are insured, it will be more secure and reliable to enter into an cooperative agreement. In this way trusted cliques can evolve. The firms benefit from connecting to other insured firms, and the insurance company can offer fair prices to the insured companies, because the risk is low trusted clique. Hence this model, although very simple, shows an insurable topology where insured agents benefit from being insured.

This model is very simplified and suffer from many limitations, among others it is too simple to reflect the dynamics of a real world scenario, where each node will have different variables with different values. Although it tries to deal with the problem of correlated risks and preventing free riders from entering the trusted clique (interdependent security problem), each node have a complete network information i.e. the problem with information asymmetry is not taken into account.

5.3 Model 2 - Including Parameters

To make the simple model more realistic, we have to create a game with parameters, that reflects some real world scenarios. The characteristics of the game is as follows: a node can be either insured or not insured, the insured ones have to pay an insurance

cost I_0. Every node starts with a fixed income, α, to further increase their income they have to establish links to other agents. For each link they establish they receive a payoff of β. This represents the positive network externalities of the game. An insured node has to pay a cost of I_l for every link he establishes. From the previous model, we the game is bidirectional, i.e. both nodes need to agree of the establishment of a link, and if both are insured, they both have to pay the cost I_l. Every agent who is not insured will have a risk of failure(infection, bankruptcy, or some other type of failure), this is captured with the expected risk cost r. Every node, insured or not who connects to a non-insured node will also suffer from this cost. The link insurance cost and the risk are negative network externalities in the game. Table 5.1 presents an overview of the parameters.

α - agents fixed income
β - income from establishing a direct link
I_o - cost of having insurance.
I_l - increased insurance cost per link the node establishes
r - expected risk cost

Table 5.1: Table showing the parameters to be used in the first model

Two agent game To begin analyzing the game, lets consider a two-person game. In this game the strategy space of both players consist of four different strategies. They can choose to purchase insurance or not, and whether or not to establish a link to the other player. I.e. the different strategies are: Be insured and establish link noted as: IL, be insured and not establish link: $I\overline{L}$. Not insured and establish link: $\overline{I}L$, and not insured and not establish link: $\overline{IL}$. It should be noted that since the decision to establish a connection is bidirectional, both have to choose a strategy where they want to establish a link, for the link to be establishment to be successful. Figure 5.2 shows the different outcomes of this game.

To be able to limit correlated risk and prevent the interdependent security problem, we want to keep following the rules from the previous model, where the insured nodes form a trusted clique is what we want to achieve. When non-insured nodes connect to each other, they both end up with this payoff 5.1. If they do not establish connection, they both receive the payoff 5.2.

$$U = \alpha - 2 * r + \beta \tag{5.1}$$

$$U = \alpha - r \tag{5.2}$$

		Agent B			
		IL	$I\overline{L}$	$\overline{I}L$	$\overline{IL}$
Agent A	IL	$\alpha+\beta-I_o-Il$ $\alpha+\beta-I_o-Il$	$\alpha-I_o$ $\alpha-I_o$	$\alpha+\beta-I_o-Il-r$ $\alpha+\beta-r$	$\alpha-I_o$ $\alpha-r$
	$I\overline{L}$	$\alpha-I_o$ $\alpha-I_o$	$\alpha-I_o$ $\alpha-I_o$	$\alpha-I_o$ $\alpha-r$	$\alpha-I_o$ $\alpha-r$
	$\overline{I}L$	$\alpha+\beta-r$ $\alpha+\beta-I_o-Il-r$	$\alpha-r$ $\alpha-I_o$	$\alpha+\beta-2*r$ $\alpha+\beta-2*r$	$\alpha-r$ $\alpha-r$
	$\overline{IL}$	$\alpha-r$ $\alpha-I_o$	$\alpha-r$ $\alpha-I_o$	$\alpha-r$ $\alpha-r$	$\alpha-r$ $\alpha-r$

Figure 5.2: Normal form game, showing the different strategies and the payoffs for the different outcomes. The payoff for agent A is written first, then the payoff for agent B is on the line beneath. An agent has a strategy space of size 4.

From this equation we see that if $r > \beta$ then no connections will be made between non-insured nodes, because they would strictly prefer the payoff from not connecting. If an insured node connects to a non-insured one, he will end up with this payoff 5.3. If he do not connect he will receive the payoff shown in 5.4.

$$U = \alpha - I_0 - I_l - r + \beta \tag{5.3}$$

$$U = \alpha - I_0 \tag{5.4}$$

If $I_l + r > \beta$ the insured one will prefer not to connect, else he would prefer to establish a connection, and since the non-insured agent is always better off when connected to an insured agent, he will accept the establishment. This can be shown when comparing the two payoffs. Payoff of connecting to an insured one: $U_i = \alpha - r + \beta$ is allways higher than not connecting: $U_i = \alpha - r$, as long as $\beta > 0$.

Multiple nodes Making the model more realistic we expanded it to apply multiple nodes. Our goal is to end up in a trusted clique of insured nodes, to achieve this we need to make sure that only insured nodes connect to each other, we want 5.4 to be larger than 5.3. I.e. This has to hold:

$$I_l + r > \beta \tag{5.5}$$

When insured nodes connect to other insured nodes, they both end up with this payoff:

$$U = \alpha - I_0 - I_l + \beta \tag{5.6}$$

To ensure that both agents will connect to each other the following has to hold:

$$I_l < \beta \tag{5.7}$$

For the game to end up as the one described earlier, where only insured nodes connect to other insured nodes, both 5.5 and 5.7 has to hold, which gives us this limitation on the parameter I_l:

$$\beta - r < I_l < \beta \tag{5.8}$$

If the cost of insuring link is between these bounds, the insured nodes will only connect to other insured nodes. This holds a game with n players, because the relative change in payoff is linear and non-dependent on number of links already established. If the condition is fulfilled the game will end up in one or two cliques. Two cliques if the non-insured nodes connect to each other, and they do so if: $\beta > r$.

In this model the network formation is done endogenously, and when following the limitation 5.8 we ensure that only insured nodes will connect, and the network ends

up in a insurable network topology. We have neglected the information asymmetry problem, because we made the assumption that all nodes can differentiate insured versus non insured nodes. This limitation makes the model less applicable to numerous real world network, however in financial transactions and in software development networks, it is reasonable to assume that the parties can acquire this type of information regarding their transactional partners. And thus they solve the information asymmetry problem by themselves, by requiring proof of insurance prior to establishing a connection. As shown, if the insurance cost is within its needed limitations, the network will evolve endogenously, and end up with a insurable-clustered component, which is beneficial for both the insurer and the nodes.

5.3.1 Scenario - meeting the conditions

By assigning values to the variables, we can show the outcome of the game in different scenarios. With the values from table 5.2, the insurance cost of establishing a link satisfies the condition in equation 5.8. If we play this game between two agents we can see the result in the normal form table 5.3. We see that the results are as we expected, insured nodes will only choose to connect with other insured nodes, they are also satisfied when not connected to each other. However, this is not the social optimal outcome, and since they have complete network information, they will choose to connect to each other, because they will both achieve a higher payoff. As described, it does not matter if we only consider a two person game, because the change in payoffs of adding a link, is linear an independent of the agents degree, and if the insurance cost is right, it will never be beneficial for a insured node to connect to a non-insured.

$\alpha = 10, \beta = 10, I_o = 5, I_l = 3, r = 8$

Table 5.2: Table showing the parameters and their assigned values

		Agent B			
		IL	$I\overline{L}$	$\overline{I}L$	$\overline{IL}$
Agent A	IL	12 ,12	5,5	4,12	5,2
	$I\overline{L}$	5,5	5,5	5, 2	5,2
	$\overline{I}L$	12,4	2,5	4,4	2,2
	$\overline{IL}$	2,5	2,5	2,2	2,2

Figure 5.3: Normal form game between two agents with the parameters given in 5.2, the best response of a player to a given strategy is marked with an underscore.There are two pure nash equilibriums in this game,IL, IL and $I\overline{L}, I\overline{L}$.

5.3.2 Scenario - violating the conditions

When setting the insurance cost: $I_l < \beta - r$ or $I_l > \beta$ we are violating the condition who ensured that only insured nodes connected to each other. In table 5.3 we let the insurance cost be: $I_l < \beta - r$, this results in the payoff matrix shown in figure 5.4. There are still the same nash equilibriums, but the interesting part is the best response of an insured agent who want to establish link, when the other agent is not insured but also want to establish link. This scenario has now changed, and we see that the insured agent would agree to the link establishment, this will result in an untrusted and thus an non-insurable topology. A game with multiple nodes, insured and non-insured, will end up in one fully connected network. On the other hand, if $I_l > \beta$, then it is easily seen that only the non-insured will connect to each other, and the insured nodes will not choose to connect to anyone because it is to expensive. Therefore to ensure that only insured agents connect to each other, equation 5.8 has to be satisfied.

$\alpha = 10, \beta = 10, I_o = 5, I_l = 1, r = 8$

Table 5.3: Table showing the parameters and their assigned values, the insurance cost of establishing link is now violating the equation 5.8

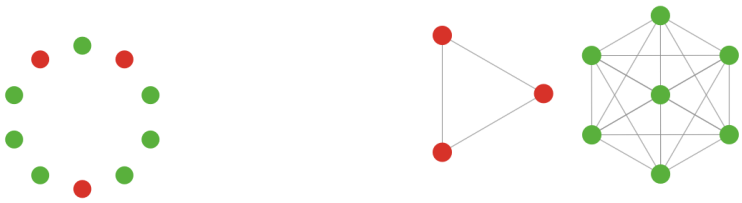
		Agent B			
		IL	$I\overline{L}$	$\overline{I}L$	$\overline{IL}$
Agent A	IL	$\underline{14}$,$\underline{14}$	5,$\underline{5}$	$\underline{6}$,12	$\underline{5}$,2
	$I\overline{L}$	5,$\underline{5}$	$\underline{5}$,$\underline{5}$	5, 2	$\underline{5}$,2
	$\overline{I}L$	12,$\underline{6}$	2,	4,4	2,2
	$\overline{IL}$	2,$\underline{5}$	2,$\underline{5}$	2,2	2,2

Figure 5.4: Normal form game between two agents with the parameters given in table 5.3, the best response of a player to a given strategy is marked with an underscore.There are two pure nash equilibriums in this game,IL, IL and $I\underline{L}, I\underline{L}$.

5.4 Simulating Model 2

To verify the result of this network formation game with multiple nodes, we performed different simulations. The network formation is performed by selecting two random nodes, not neighbouring each other, then both nodes checks whether they would prefer to establish a connection or not. The rules are as described earlier, when a

node is considering establishing a link it chooses to do so if the payoff received is larger than the payoff he already poses, and the decision is bilateral. In the simulator a node is insured with a probability, p. This selection is repeated until the network are fully connected or no more nodes are willing to establish new connections. By selecting nodes at random and checking if both of them would like to connect to each other, we relax the assumption of full network information, because now nodes only get to know if another node is insured or not, by asking them.



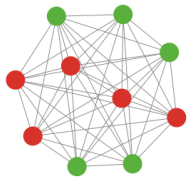
(a) Ten nodes randomly, with probability 0.5, chosen to be either insured (green) or non-insured (red.

(b) Two clustered fully connected networks. One consisting of insured agents the other consists of non-insured. The link establishment is done by following the rules described above

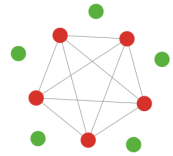
Figure 5.5: The figure shows how ten nodes start out with no links, and then add links as long as they can increase their payoff, the result are two seperate cliques, one consisting of non-insured and the other of insured nodes.

Simulation of game with optimal parameters In figure 5.5 we see the result of a simulation with the parameters from table 5.2. Since these parameter values holds for the condition 5.8, the game should end up in two cliques, one with insured nodes and another with non-insured. The result are shown in figure 5.5b, and confirms our calculations where only insured nodes connect to each other. In this figure there are only included $n = 10$ nodes, this is done to make the figure readable and easy to understand. The same results where obtained when performing the simulation with larger values of n, however the resulting printouts was very complex and chaotic.

Simulation of game with parameters violating equation 5.8 In this simulation, the cost of insuring a link where violating the equation 5.8. The result can be seen in figure 5.6. In figure 5.6a we see the result when $I_l < \beta - r$, the result is one clique of both insured and non-insured nodes. In figure 5.6b the insurance cost is $I_l > \beta$, and as we see only non-insured nodes connect to each other, because the insurance cost per link cost more than the benefit given from connecting to a new node, i.e. the insured ones choose not to establish any connections.



(a) Ten nodes insured with probability 0.5, and the parameters from table 5.3. The link insurance cost, I_l, is violating the condition in equation 5.8, and the resulting network is one clique of both insured and non-insured nodes.



(b) Ten nodes insured with probability 0.5, with parameters from table 5.3, except that the link insurance cost was:, $I_l = 11 > \beta$. This resulted in a clique of only non-insured nodes.

Figure 5.6: The figure shows the two possible scenarios that violates the equation 5.8, 5.6a shows the result when $I_l < \beta - r$ and 5.6b shows the result when $I_l > \beta$.

5.5 Model 3 - Including maximum node degree and bonus

We keep adding new features to the model, here we introduce a maximum node degree per node, and a payoff bonus when reaching this level. This is done to make a more applicable model in certain scenarios. For example, lets consider a software company who want to develop a new product. However, they do not have the required resources or knowledge to complete the product, and will therefore need help from other companies with the desired knowledge or resources. When the product is finished the company get paid, but not before, to finish the product they need to cooperate with others. To model this scenario we added a bonus γ, which represents the payoff when a node reach their desired number off established connections, i.e. their maximum node degree(m). Except from this fact the game is as before, nodes connect to other nodes if they can reach a higher payoff by doing so.

Four different scenarios

To further analyze this model, lets take a closer look on the four different scenarios of the game, a insured node wants to connect to another insured node, insured tries to connect to a non-insured node, non-insured tries to connect to another non-insured node, and non-insured who tries to connect to a insured node.

Insured to insured When an insured node tries to connect to another insured node, the node decision depends on whether he can increase his payoff. Let U_i denote the payoff of a node with node-degree i. When adding a link the payoff the node

receives is as follows:

$$U_{i+1} = \begin{cases} \alpha + \beta - I_0 - I_l, & \text{if } i = 0 \\ U_i + \beta - I_l, & \text{if } i > 0 \\ U_i + \beta - I_l + \gamma, & \text{if } i = m \end{cases} \tag{5.9}$$

For insured nodes to connect to each other, $U_{i+1} > U_i$. This model is very similar to the earlier model, but we need to consider the received bonus when reaching the maximum node degree, m. We model this by adding, the bonus divided on the current degree, in the decision process of establishing link or not.

$$\begin{aligned} U_i + \beta - I_l + \frac{\gamma}{m-i} &> U_i \\ \beta - I_l + \frac{\gamma}{m-i} &> 0 \\ \rightarrow \quad \beta + \frac{\gamma}{m-i} &> I_l \end{aligned} \tag{5.10}$$

It should be noted that the actual bonus is not added to the current payoff before the node reach the maximum degree, as shown in equation 5.9. The equation $\frac{\gamma}{m-i}$ reflects the expected payoff from taking the risk of establishing a connection. This value increases linearly according to how close you are to reach m. In this way the model will change from the former models, because now the nodes have more incentive to connect to other nodes, and in some scenarios they will be willing to take the risk of connecting to a non-insured node in order to reach the expected bonus. The model now introduces a risk factor, because it is not certain that the nodes will obtain enough links, and if not, they will not receive their bonus, however they are stuck with the established connections.

Insured connect to non-insured The payoff an insured node receives in this scenario is as follows:

$$U_{i+1} = \begin{cases} \alpha + \beta - I_0 - I_l - r, & \text{if } i = 0 \\ U_i + \beta - I_l - r, & \text{if } i > 0 \\ U_i + \beta - I_l - r + \gamma, & \text{if } i = m \end{cases} \tag{5.11}$$

To establish a connection from an insured node to a non-insured one, the following has to hold:

$$\begin{aligned} U_i + \beta - I_l - r + \frac{\gamma}{m-i} &> U_i \\ \beta - I_l - r + \frac{\gamma}{m-i} &> 0 \\ \rightarrow \quad \beta + \frac{\gamma}{m-i} - r &> I_l \end{aligned} \tag{5.12}$$

Non-insured to non-insured When a non-insured node connect to another not-insured node this is the payoff they receive:

$$U_{i+1} = \begin{cases} \alpha + \beta - r, & \text{if } i = 0 \\ U_i + \beta - r, & \text{if } i > 0 \\ U_i + \beta - r + \gamma, & \text{if } i = m \end{cases} \tag{5.13}$$

To establish the connection this equation has to hold:

$$\begin{aligned} U_i + \beta - r + \frac{\gamma}{m-i} &> U_i \\ \beta - r + \frac{\gamma}{m-i} &> 0 \\ \rightarrow \quad \beta + \frac{\gamma}{m-i} &> r \end{aligned} \tag{5.14}$$

Non-insured to insured

$$U_{i+1} = \begin{cases} \alpha + \beta, & \text{if } i = 0 \\ U_i + \beta, & \text{if } i > 0 \\ U_i + \beta + \gamma, & \text{if } i = m \end{cases} \tag{5.15}$$

As we see, this is a strictly increasing function, and thus a non-insured will always connect to an insured node if given the option, and as long as β is positive, which it is, given the rules of the model.

Limitations to ensure a clique of only insured We are interested in finding insurable topologies, one candidate is a sub graph consisting of only insured nodes. By analyzing the different scenarios above we can find limitations on the cost of insuring a link, that will force the network formation game to end up in an insurable sub graph. We know that an insured node would want to connect to another insured node if the equation 5.10 is satisfied. In the equation we see that the expected bonus per established link is increasing, i.e. if an insured node of degree zero is willing to connect to another insured node, then every node with a degree higher than zero also would like to connect to another insured node. Thus to ensure that insured nodes connect to each other this equation has to hold:

$$\beta + \frac{\gamma}{m} > I_l \tag{5.16}$$

We also want to ensure that insured nodes never establishes links with non-insured nodes, from 5.11 we see that this has to hold:

$$\beta + \frac{\gamma}{m-i} - r < I_l \tag{5.17}$$

This can be simplified, since we know the insured nodes with degree $m-1$ get the highest expected bonus when establishing a new link, i.e. if we can ensure that nodes

with this degree do not establish links to non-insured nodes, we also know that every node with degree less than $m-1$ will not establish links to non-insured nodes. From this we get the equation:

$$\begin{aligned} \beta + \frac{\gamma}{m-(m-1)} - r &< I_l \\ \rightarrow \quad \beta + \gamma - r &< I_l \end{aligned} \tag{5.18}$$

To summarize, the equations 5.16 and 5.17 gives the final limitation on the link insurance cost:

$$\beta + \gamma - r < I_l < \beta + \frac{\gamma}{m} \tag{5.19}$$

Additionally, in order to make it possible for the game to end up in an insurable topology equation 5.20 has to be satisfied. As we see from the equation, if the risk to bonus ratio gets to small it gets more and more unlikely to ensure an insurable topology. If we think about a real world scenario where you get a bonus for establishing a fixed number of equations, you would be more willing to take a risk if the possible reward of doing so is large, this is what this equation express.

$$\begin{aligned} \gamma - r &< \tfrac{\gamma}{m} \\ 1 - \frac{r}{\gamma} &< \tfrac{1}{m} \\ \rightarrow \quad 1 - \frac{1}{m} &< \tfrac{r}{\gamma} \end{aligned} \tag{5.20}$$

5.5.1 Simulations

We simulate how networks form when the conditions from equation 5.19 are met, and what happens when they are not. In addition we use the simulation to look at the consequences with regards to the payoff, when the required number of connections aren't met.

Simulation when conditions are met First we simulate a network formation game when the link insurance cost satisfied the equation 5.19, using the parameters in table 5.4. As we see in figure 5.7 the results where as expected, the cost of

$\alpha = 10, \beta = 10, I_o = 5, I_l = 9, r = 8, \gamma = 5, m = 5$

Table 5.4: Parameters used in the simulation

insuring a link satisfied the conditions found earlier and thus the result where two cliques, one consisting of only insured and the other of non-insured nodes.

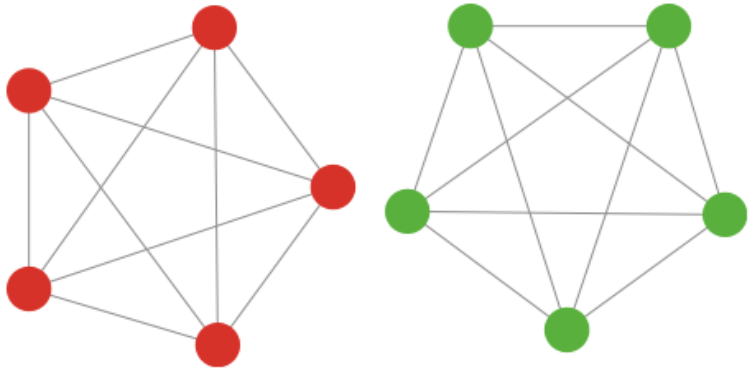


Figure 5.7: Two clustered fully connected networks, created by simulating with the parameters from table 5.4 One consisting of insured agents the other consists of non-insured.

Simulation when the parameters violates the conditions If we change the link insurance cost, so it is just below the limit, $I_l = 6$, the result is quite different as depicted in figure 5.8. Here we see that eventhough non-insured nodes can fail and accumulate negative payoff, some of the insured nodes have taken a risk by connecting to non-insured nodes in order to receive the bonus.

Consequences of not reaching required number of edges Both of these scenarios ends up in a situation where the nodes reach their maximum node degree and they all receive the bonus. However each time a node chooses to connectio to another node, except when $i = m - 1$, it does not know whether it will reach the maximum node degree. Hence the node might take a risk of connecting to other nodes without being able to reach their required number of connections. This means that in certain situation one might end up getting a total $i < m$ connections which results in a much lower payoff than expected. If the variables are set close to a worst-case, such as in table 5.5 , we end up with two cliques with payoffs close too or worse than the payoff each node had initially.

$\alpha = 10, \beta = 10, I_o = 5, I_l = 11, r = 8, \gamma = 25, m = 8$

Table 5.5: Parameters used in simulation

With the variables from table 5.5 the resulting payoffs from figure 5.9 equals 6 for each of the non-insured nodes and -1 for the insured nodes. In comparison, the same figure using the variables from table 5.4 results in a positive payoff 15 for each of the nodes in the insured clique. This comparison shows the consequences of failing

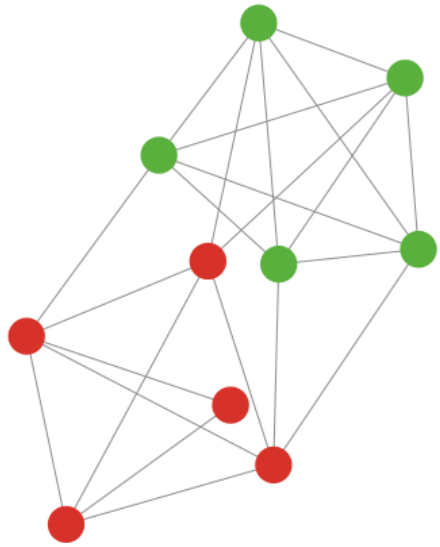


Figure 5.8: Simulation when the cost of insuring a link is just below the limits.

to achieve the required amount of connections, which might be the case if a company is trying to complete a project which requires too many external suppliers.

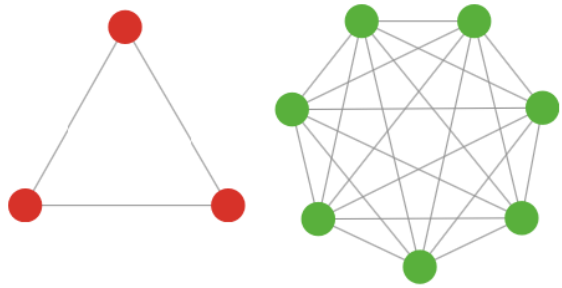


Figure 5.9: Simulation when the cost of insuring a link is just below the limits and the maximum node degree is high.

5.6 Model 4 - Including bulk insurance discount

Insurance companies often interpret a quantum discount when purchasing multiple products. From convenience stores we are used to the slogan "buy one get one for free". It seems to be common for insurance companies to offer discount to their customers if they choose to collect some or all of their insurances with them. Several insurance companies in Norway, such as Sparebank 1 offers customers up to 25 % discount according to the following rules [Spa].

- 10% discount if the person has signed three different insurances
- 15% discount if the person has signed four different insurances
- 20% discount if the person has signed five or more different insurances
- Plus additional 5% discount if the person is a customer of the bank.

The insurance offered is intended to the individual market and includes among others: travel insurance, household insurance, car insurance, house insurance, insurance of valuable items and yacht insurance. Since this seems to be the trend for marketing insurance products, it is reasonable to believe that several bonus options would be included in a cyber-insurance product. Since our model so far reflects that a company have to insure each of the connections to other nodes in their network, it is assumed that a similar discount rate following the number of established would be implemented.

How insurance companies choose to formulate their discount rate might vary. One solution might be to follow a strict 5% discount per new connection, similar to the one from Sparebank 1, or let the discount follow a power law. However, we choose to follow a discount rule which directly reflects the number of connections the company have established. The price for adding a new connection follows the equation:

$$\frac{I_l}{i+1} \tag{5.21}$$

Here, i is the current number of established connections. This means that the more connections a company acquire the cheaper the connections will be. If we add

the new rule to the equation 5.9 which shows the connection between two insured nodes, we get the following equations:

$$U_{i+1} = \begin{cases} \alpha + \beta - I_0 - I_l, & \text{if } i = 0 \\ U_i + \beta - \frac{I_L}{i+1}, & \text{if } i > 0 \\ U_i + \beta - \frac{I_L}{i+1} + \gamma, & \text{if } i = m \end{cases} \tag{5.22}$$

As described, for insured nodes to connect to each other, $U_{i+1} > U_i$. Building on the already existing model, the quantum discount slightly changes the decision process:

$$\begin{aligned} U_i + \beta - \frac{I_l}{i+1} + \frac{\gamma}{m-i} &> U_i \\ \beta - \frac{I_l}{i+1} + \frac{\gamma}{m-i} &> 0 \\ \beta(i+1) + \frac{\gamma}{m-i} &> \tfrac{I_l}{i+1} \\ \rightarrow \qquad \beta(i+1) + \frac{\gamma(i+1)}{m-i} &> I_l \end{aligned} \tag{5.23}$$

Similar calculation can be done for the other three scenarios in the game, and they all result in almost the same outcome. First of all results from having quantum discounts on new connections results in a overall higher payoff for the nodes, as long as $i > 1$. Since the cost of insuring a new link becomes cheaper. This means that the nodes will have a higher incentive to create links to each other, because the left side of equation 5.23 yields a higher payoff than before. Which leads to a consequence that more insured nodes could connect to non-insured nodes. Building on the final condition 5.19 in previous section, we now get:

$$\begin{aligned} \beta + \gamma - r < \frac{I_l}{i+1} < \beta + \frac{\gamma}{m} \\ \beta(i+1) + \gamma(i+1) - r(i+1) < I_l < \beta(i+1) + \frac{\gamma(i+1)}{m} \end{aligned} \tag{5.24}$$

From equation 5.24 we see that the initial variable $I_(l)$ has to be priced higher, in order to ensure that only insured nodes connects to other insured nodes. However, beside this drawback, we also experience some positive effects from the modification, since the the purchase of more connections is cheaper the product might be more attractive for potential customers.

5.6.1 Game with incomplete information

In this game we have included the problem of information asymmetry, this is done by letting nature selecting whether a player is insured or not, a player is insured with probability p, and not insured with probability $1-p$. The game is as earlier, link establishment is a bilateral decision, and we select two random nodes each round, and check if they would like to connect to each other. The difference is that we have inserted information asymmetry, only player 1 knows the type of the other player. Both players knows their own type, but player 2 only have a belief about the type of player 1.

5.6.2 Calculating the different equlibriums

In this game we have two types of players, type 1 ($t1$): insured and type 2 ($t2$): not insured. Player 1's type is chosen randomly by nature, with probability p of being type 1 and $1-p$ of being type 2. In this two person game player 1 have complete

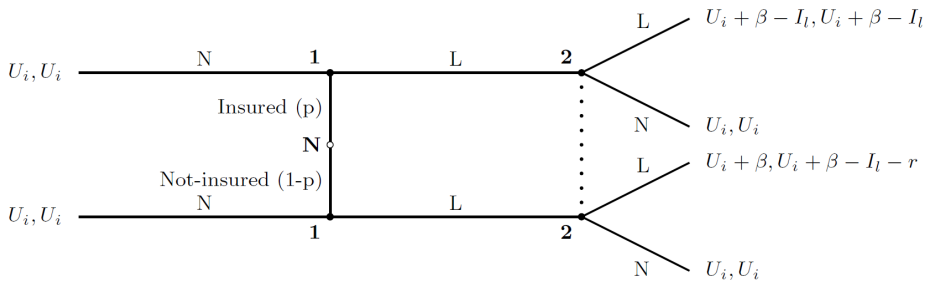


Figure 5.10: Signalling game with two players, player 1's type choosen by nature, player2 is insured. Player 1 have complete information, player 2 suffer from incomplete information, and act on beliefs.

information, i.e. he knows his own and the other players type. Player 2 suffer has incomplete information and only knows his own type. In the extensiveform shown in figure 5.10, we see that $t2's$ strategy L dominates N, and thus $t2$ will never play N.

Separating equilibrium If we can find a separating equilibrium, this will enable player 2 to distinguish the two possible types of player 1. Since player 1 will never play N as type 2, there are only one possible separating equlibrium, type 1 plays L and type 2 plays N. Hence player 2's beliefs are as in equation 5.25.

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ N, & \text{if } t2 \end{cases} \tag{5.25}$$

Let $\mu_1(t_i|N)$, denote the probability that player 1 is of type t_i. And by using bayes rule we get this equation:

$$\mu_1(t_1|N) = \frac{P(N|t_1)P(t_1)}{P(N)} = \frac{P(N|t_1)P(t_1)}{P(N|t_1)P(t_1) + P(N|t_2)P(t_2)} \tag{5.26}$$

And with player 2's belief, we get that $\mu_1(t_1|N) = 1$ and $\mu_1(t_2|L) = 1$. Now we calculate player 2's expected utility from playing L and N:

$$\begin{aligned} EU_2(L,L) &= \mu_1(t_1|L)U_2(L,L;t_1) + \mu_1(t_2|L)U_2(L,L;t_2) \\ \rightarrow \qquad & EU_2(L,L) = U_i + \beta - I_l - r \qquad (5.27) \\ EU_2(N,L) &= \mu_1(t_1|L)U_2(N,L;t_1) + \mu_1(t_2|L)U_2(N,L;t_2) \\ \rightarrow \qquad & EU_2(N,L) = U_i \qquad (5.28) \end{aligned}$$

From these two equations we see that the best response of player 2(BR_2) when he observes the other player choosing action L is:

$$BR_2(L) = \begin{cases} L, & \text{if } \beta - r \geq I_l \\ N, & \text{if } \beta - r < I_l \end{cases} \tag{5.29}$$

Player 2's expected utility when type 1 chooses N, is easily seen to be U_i. To confirm if this is a separating equilibrium we must see if player 1 has any incentive to deviate from the strategies in player 2's belief. Type 2 will never deviate, so lets investigate type 1. For player 1 to be willing to play N when he knows player 2's best response function, this must hold: $\beta < I_l$. If this is true, then player 2's best response is to play N. I.e. the only separating equilibrium is the following:

$$\beta < I_l \tag{5.30}$$

$$\sigma_1 = \begin{cases} L, & \text{if } t1 \\ N, & \text{if } t2 \end{cases} \tag{5.31}$$

$$BR_2(\sigma_1) = N \tag{5.32}$$

This means that in a separating equilibrium, the game will end up with no link establishment.

Pooling equilibrium In a pooling equilibrium player 2 will not be able to distinguish the two types, and since $t1$'s strategy L dominates N, i.e. there is only one possible equilibrium, the one where both types of player 1 plays L.

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{5.33}$$

By using bayes rule we get that $\mu(t_1|L) = p$ and $\mu(t_2|L) = 1 - p$. Player 2's expected utility is then:

$$EU_2(L, L) = p(U_i + \beta - I_l) + (1 - p)(U_i + \beta - I_l - r)$$
$$\rightarrow \quad EU_2(L, L) = U_i + \beta - I_l - r + r \tag{5.34}$$
$$EU_2(N, L) = U_i \tag{5.35}$$

From this we get player2's best response:

$$BR_2(L) = \begin{cases} L, & \text{if } \beta + rp - r \geq I_l \\ N, & \text{if } \beta + rp - r < I_l \end{cases} \tag{5.36}$$

By using this best response function, player 1 sees that as long as $\beta > I_l$ he will never deviate from player 2's beliefs. And it is a pooling equilibrium where both player choose L, as long as $\beta > I_l$ and $\beta + rp - r > I_l$. We also know that this: $rp - r < 0$ is allways true, and thus the only pooling equilbrium is the one where both players plays L, and the condition for this is: $\beta > I_l$.

Player 2 not insured, player 1's type choosen by nature The rules of the game are as before, the only thing that has changed is the type of player 2, and thus the payoffs are different and we need to see if there exists separating and pooling equilibrium in this game as well.

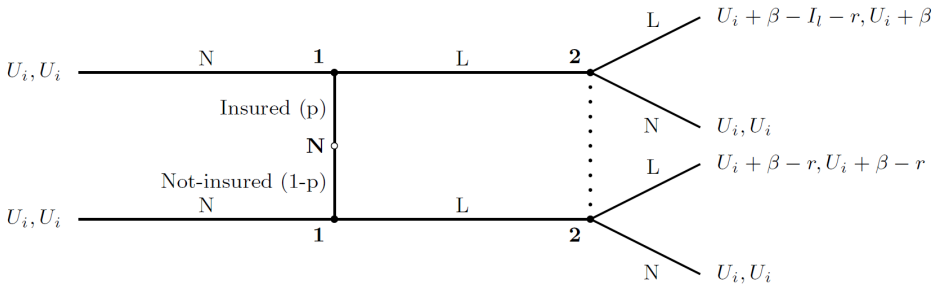


Figure 5.11: TESTESTTEST

Separating equilibrium In this game there is no dominant strategy for player 1, thus we have to check for the two possible separating equilibriums. We start with the separating equilibrium with the beliefs shown in equation 5.37.

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ N, & \text{if } t2 \end{cases} \tag{5.37}$$

With the beliefs in equation 5.37, this is his expected payoffs:

$$EU_2(L, L) = (U_i + \beta) \tag{5.38}$$
$$EU_2(N, L) = (U_i) \tag{5.39}$$

From this we see that his best response when player 1's action is L, is to allways play L:

$$BR_2(L) = L \tag{5.40}$$

To see if this is an equilibrium, we have to see if player 1 has any incentive to deviate. Lets check for the two types of player 1: If $\beta > r$ then type 2 would deviate, because he could achieve a higher payoff by playing L, given the beliefs of player 2 in equation 5.37. So we know that for this to be an equilibrium,

$$\beta < r \tag{5.41}$$

When analyzing from player 1 type 2's perspective, for him to play L, this has to hold: $U_i + \beta - I_l - r > U_i$. The only way this can hold is if $\beta > I_l + r$. We see that equation 5.41 is violating this condition, and thus we have no separating equilibrium with the beliefs in equation 5.37. Now lets look at the other possible separating equilibrium, see equation 5.42.

$$\sigma_1(t_i) = \begin{cases} N, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{5.42}$$

Player 2's expected payoffs are as follows:

$$EU_2(L, L) = U_i + \beta - r \tag{5.43}$$
$$EU_2(N, L) = U_i \tag{5.44}$$

From this we get the best response function:

$$BR_2(L) = \begin{cases} L, & \text{if } \beta \geq r \\ N, & \text{if } \beta < r \end{cases} \tag{5.45}$$

For this to be a separating equilibrium, we need to see if player 1 would deviate from player 2's beliefs. Type $t1$ will not deviate as long as $\beta < I_l + r$. Type $t2$ will not deviate if $\beta \geq r$, if this condition is true, we see that player 2 will play L. I.e. the only separating equilibrium that exists is when player 2 plays L, player 1 of type $t1$ plays N and player 1 of type$t2$ plays L. And for this to happen we get this condition on β.

$$I_l + r > \beta > r \tag{5.46}$$

Pooling equilibrium Two possible, one where both types of player 1 plays L, and one where both types plays N. Lets first analyze the one where both types of player 1 plays L.

$$\sigma_1(t_i) = \begin{cases} L, & \text{if } t1 \\ L, & \text{if } t2 \end{cases} \tag{5.47}$$

With the beliefs shown above, player 2's expected payoffs are:

$$EU_2(L) = p(U_i + \beta) + (1-p)(U_i + \beta - r)$$

$$EU_2(L) = U_i + \beta - r + pr \tag{5.48}$$

$$EU_2(N) = U_i \tag{5.49}$$

From this we get the best response function :

$$BR_2(L) = \begin{cases} L, & \text{if } \beta \geq r - pr \\ N, & \text{if } \beta < r - pr \end{cases} \tag{5.50}$$

Will player 1 deviate knowing this? Type $t1$ will not deviate as long as: $\beta - I_l \geq r$. And type $t2$ will not deviate as long as $\beta > r$. From this we get this final condition, if $\beta - I_l \geq r$ then there exists a pooling equilibrium where both types of player 1 plays L and player 2 also play L. From this we can also see that the other pooling equilibrium where both types of player 1, plays N, can only happen when $\beta < r$ and $\beta < I_l + r$.

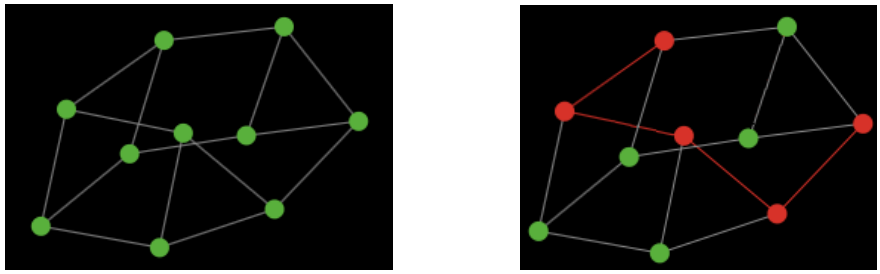
Summary When the game is suffering from incomplete information, we are not able to ensure that the network formation game end up in an insurable clique. We found one equilibrium where the non-insured player 2 where able to separate the two types of player 1, and when $\beta > r + I_l$ the resulting network is a clique of only non-insured nodes. We also found pooling equilibriums where both types of player 1 and player 2 will connect to both non-insured and insured nodes.

.....FROM HERE, it's only notes.....

5.7 DETTE ET ANNET STED KANSKJE? BLIR LITT RART Å HOPPE INN I DET HER

By adjusting the parameter one can assure that only insured agents connects to other insured agents, and the opposite, that only uninsured agents connects to each other. Hence as we can see from the figure 5.12 clustered networks of insured agents (red) are created, and as the paper [Blu11] showed, these clustered trusted networks, can achieve higher, super-critical, payoff by increasing their node degree past the critical point.

, because the nodes can thus receive a super-critical payoff, and they are also insured against contagious risk.



(a) Initial graph with 10 agents. (b) Insured agents (red) forms a network

Figure 5.12: shows how insured agents connects with each other to form a network to achieve super-critical payoffs.

Figure 5.13 presents the individual payoffs in a formation game between two agents in the described model. It is assumed that both agents has to have a desire to establish a connection in order to create a link between them. This is reasonable since a company would not prefer to enter into an agreement with negative expected payoff. As in this case would be the result when an insured agent is requested a connection with someone without insurance.

		Firm B			
		Il	$I\overline{l}$	$\overline{I}l$	$\overline{I}\overline{l}$
Firm A	Il	$\alpha+\beta-I_o-Il$ $\alpha+\beta-I_o-Il$	$\alpha-I_o$ $\alpha-I_o$	$\alpha+\beta-I_o-Il-r*q$ $\alpha+\beta-r*q$	$\alpha-I_o$ $\alpha-r*q$
	$I\overline{l}$	$\alpha-I_o$ $\alpha-I_o$	$\alpha-I_o$ $\alpha-I_o$	$\alpha-I_o$ $\alpha-r*q$	$\alpha-I_o$ $\alpha-r*q$
	$\overline{I}l$	$\alpha+\beta-r*q$ $\alpha+\beta-I_o-Il-r*q$	$\alpha-r*q$ $\alpha-I_o$	$\alpha+\beta-2*r*q$ $\alpha+\beta-2*r*q$	$\alpha-r*q$ $\alpha-r*q$
	$\overline{I}\overline{l}$	$\alpha-r*q$ $\alpha-I_o$	$\alpha-r*q$ $\alpha-I_o$	$\alpha-r*q$ $\alpha-r*q$	$\alpha-r*q$ $\alpha-r*q$

Figure 5.13: Normal form game between two agents individually choosing to purchase insurance and express desire to connect to the other [1]

If we give value to the variables in figure 5.13 one can observe the model's different equilibrium's. It is difficult to know exactly how the variables are set and this would vary considerably between different markets. In a real worlds scenario the variables would also be different for each agent. However in figure 5.14 we decided to set a fixed value (which is assumed to be corresponding to the real values) for each variable in order to show a concept of how cyber-insurance can be used to create beneficial payoffs. The following values where used: $\alpha = 10$, $\beta = 10$, $I_o = 5$, $I_l = 2$, $r = 20$, $q = 0.5$.

From the payoff matrix 5.14 we observe two different Nash equilibrium's: One when both agents are insured and wants to connect to the other agent, and one when both are insured but does not want to establish a connection. These are the

[1] A link will only be created if both agents wishes to establish a connection.

		Agent B			
		IL	$I\overline{L}$	$\overline{I}L$	$\overline{IL}$
Agent A	IL	12 ,12	5,5	4,12	5,2
	$I\overline{L}$	5,5	5,5	5, 2	5,2
	$\overline{I}L$	12,4	2,5	4,4	2,2
	$\overline{IL}$	2,5	2,5	2,2	2,2

Figure 5.14: Shows equilibrium's in the resulting payoff matrix.

possible outcomes between the two agents, however as we can see it the social optimal solution would be for two insured agents to connect with each other, i.e they would both receive a significantly higher payoff. This demonstrates that a cluster of insured nodes would achieve higher payoffs.

5.8 Game including max node degree

FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF So far the model describes a scenario where the goal is to get all the insured nodes to connect with each other. As we have seen this creates a strong trusted environment for the insured nodes when the parameters are adjusted to certain values. However, in many scenarios the goal might not be to be connected to everyone. Sometimes a company wishes to reach a specific number of connections in order to receive a significant profit, which is denoted γ. Such scenario might create incentives for insured nodes to connect with non-insured, in order to reach the desired number of connections. As an example consider a software company wanting to implement a new software program, however they do not have the capacity or resources to do it alone. Their goal is to establish enough partnerships to be able to create the new program. In this game we might end up in a situation where insured agents are willing to connect with non-insured, to reach the desired number of partners. Table 5.6 summarizes the added parameters.

m - an agents desired number of connections
n - an agents number of established connections L_i - connections with insured agents
L_{ni} - connections with non-insured agents
γ - an agents profit from reaching m

Table 5.6: Table showing the parameters added to the model

Building on the already existing model this model adds the property of a significant bonus γ if a desired number of links m are established. From here we can describe two different models, one where the insured agent first tries to connect with other insured agents, however if there are not enough insured agents it will try to establish connections with non-insured agents. The other model shows a game where the insured agent is less strict on whether the other node is insured or not. The insured agent makes a decision with regards to the equation 5.52. Here $\frac{\gamma}{L_{ni}}$ will increase as more connections are established. I.e. the more established connections the higher probability for the insured agent to connect to a non-insured agent.

5.8.1 Game random connection

As described we now have possibility that insured and non-insured agents will establish a connection. This means that γ has to be reflected in the equation relating to whether nodes, insured or not will connect. To simplify the scenario we assume that each new connection contribute with an extra $\frac{\gamma}{m-\#l}$, which reflects an expectation of reaching m connections, hence we end up with the following equations for the new game:

Insured connects to insured:

$$U_{i+1} = U_i - I_l + \beta + \frac{\gamma}{m - \#l} \tag{5.51}$$

Insured connects to not insured

$$U_{i+1} = U_i - I_l - r + \beta + \frac{\gamma}{m - \#l} \tag{5.52}$$

not insured connects to insured

$$U_i = U_i + \beta + \frac{\gamma}{m - \#l} \tag{5.53}$$

Not insured connects to not insured

$$U_i = U_i - r + \beta + \frac{\gamma}{m - \#l} \tag{5.54}$$

Each agent now has to evaluate whether it is beneficial to connect to a non-insured agent or not. Our goal is to be able to force that only insured nodes will connect to other insured nodes. The problem in this game is how to handle the γvaiable. The equation $\frac{\gamma}{m-\#l}$ reflects that the likelihood of reaching m connections, and the bonus profit increases linearly with the nodes number of own connections, $\#l$. If we evaluate the game we will end up with the following scenario:

A insured node will not connect to a noninsured node if the equation is met:

$$I_l > \beta - r + \frac{\gamma}{m - (m-1)} = I_l > \beta - r + \gamma \tag{5.55}$$

In addition the cost of establishing the new link, also has to be low enough for the transaction to the profitable. This means that I_l also has to be:

$$I_l < \beta + \frac{\gamma}{m)} \tag{5.56}$$

This means to ensure that only insured nodes connects to other insured nodes, and still have a profitable result I_l has to follow this equation:

$$\beta + \frac{\gamma}{m} < I_l < \beta - r + \gamma \tag{5.57}$$

5.8.2 Game connecting to insured first

Insured agents still prefer to connect to other insured agents, however, if it is not possible they will consider connecting to non-insured. As we see from equation 5.58 insured agents will have to establish L_{ni} connections to non-insured agents in order to receive γ.

$$L_{ni} = m - L_i \tag{5.58}$$

An insured agent will only connect with an non-insured agent if the following is fulfilled:

$$\frac{\gamma}{L_{ni}} > r + I_l \tag{5.59}$$

In addition the agent has to ensure that $non{-}insured\ agents\ willing\ to\ connect \geq L_{ni}$, else one will end up in a scenario where the agent takes unnecessary risk without being able to receive γ at the end. This means that the insured agent only consider connecting to other non-insured nodes if and only if it is guaranteed that the desired number of connections will be met.

Chapter 6
Relatedwork

6.1 Towards Insurable Network Architectures

[BS10] A trusted component or system is one you can insure. Cyber insurance gives an incentive to better secure your network, and will thus reduce the overall threat for both first and third parties. It will also promote gathering and sharing of information related to security incidents. All in all this will increase the social welfare by decreasing the variance of losses. But even if cyber insurance seems very profitable for everyone, it has failed to evolve as much as expected. Some reasons for this, could be:

- lack of data to calculate premium.
- Underdeveloped demand due to missing awareness for cyber risks.
- legal and procedural hurdles in substaining claim.

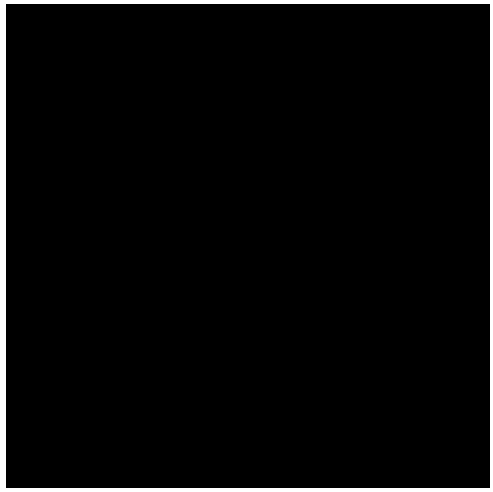


Figure 6.1: A figure

A more economic model to describe why cyber insurance is still such a niche market.

Interdependent security Expected loss due to security breach at one agent is not only dependent on this agents lvl of security, but also by other agents security investment. A good example is spam, it is dependent of number of compromised computers. This also generates an externality and encourages to free riding. which then leads to underinvestment in security.

Correlated risks Many systems share common vulnerabilities, which can be exploited at the same time. This leads to a more likely occurrence of extreme and catastrophic events, which will result in uneconomical supply of cyber insurance.

information asymmetry Since measuring security strength is very hard, people have a high incentive for hiding info. This leads to information asymmetry. All these three form a triple obstacle, which eliminates the market in evolving. All these obstacles evolve from what makes ICT succeed, distribution, interconnection, universality and reuse. This is why Architecture matters. The obstacles does not arrive from properties of individual agents, but from integration and interaction in networking. Networking is not just physical, but a abstract structure mapping physical, logical and social interconnection. A good example is development tool chains. A web-browser is not just dependent of the security the developers have implemented, but also the security in the tools used, such as libraries. Topology determines to which extet a market for cyber-insurance is affected by interdependent security. Architecture of distributed systems is not given by nature, we can change it to the better. How to design a distributed system in an insurable way? These three problems have never been analysed together, this is what this paper contributes with.

How can economic and actuarial risk models be used to guide the design of more resilient distributed systems?

How to estimate a coefficient of the strength of interdependent security?

Architecture of large distributed systems is the result of many individual agents decisions. Therefore it is hard impose a more resilient(insurable) architecture on the agents. What if we give the agents incentives to form this network instead? i.e. setting incentives for individual agents to influence their private decisions towards more resilient social outcome. (Field: endogenous network formation)

Uses GT to model incentives of the different agents.

6.2 Cyber insurance as an Incentive for Internet Security

[BL08] so far the risk management on the internet has involved methods to reduce the risks(firewalls, ids, prevention etc.) but not eliminate risk. Is it logical to buy insurance to protect the internet and its users. An important thing to notice when insuring internet, is that the entities on the internet are correlated, which means insurance claims will likely be correlated. Risks are interdependent, decision by an entity to invest in security affects the risks of others. Key result: using insurance would increase the overall security. Act as an powerful incentive, which pushes entities over the threshold where they invest in self-protection. Insurance should be an important component of risk management in the internet.

Four typical options available in the face of risks. 1. avoid the risk 2. retain 3. self protect and mitigate 4. transfer the risk. Most entities in the internet have choses a mix of 2 and 3. This has lead to lots of systems trying to detect threats and anomalies(both malicious and accidental) and to protect the users and the structure from these. but this does not eliminate risk, threats evolve over time and there is allways accidents. How to handle this residual risk? Option 4, transfer the risk to another entity who willingly accept it(hedging), insure in exchange for a fee. Allows for predictable payouts for uncertain events. But does this makes sense for the internet, benefits, to whom? and to what extent?

How to model insurance and computing premiums. avoid ruin the insurer. Actuarial approach. Economic approach: premium should be negative correlated to the amount invested in security by the entity. Users can chose to invest c or not in security solutions. Shown that in the 2 user case in absence of insurance, there is a NE in a good state, if c is low enough. These result have been extended to a network setting. This paper starts out by adding insurance to the two person game, then the n-users network, where damages spread among the users. They show that if premium discriminates about investment in protection. Insurance is a strong incentive to invest in security. Also show how insurance can be a mechanism to facilitate the deployment of security investments by taking advantage network effects such as treshold or tipping point dynamics. Uses simple models.

Using cyber insurance as a way to handle residual risk started out early in the 90's. Software and insurance sold as packages. More recently insurance companies started offering standalone products. A challenging problem is the correlation between risks, interdependent risks(risk that depend on the behavior of others).

6.2.1 Classical model for insurance

agents try to maximize some kind of expected utility function, and are risk averse. $u[w_0 - \pi] = E[u[w_0 + X]]$

Investments for an agent is either self protect and or insurance. If insurance premium is not negatively correlated to the self protection, we get moral hazard. Because if not, insurance will disincourage self protection. In this way insurance can co-exist with selfprotection.

6.2.2 Interdependent security and insurance

In presence of interdependent risks, the reward for a user investing in self-protection depends on the security in the rest of the network. Discrete choice, invest or not. loss occurs directly or indirectly. Cost of investing is c. This avoids the direct loss completely. In summary, insurance provides incentives for a small fraction of the population to invest in self-protection, which in turn induces the rest of the population to invest in self-protection as well, leading to the desirable state where all users in the network are self-protected. Furthermore, the parameter y provides a way to multiply the benefits of insurance, by lowering the initial fraction of the self-protected population needed to reach the desirable state. This paper shows that insurance provides significant benefits to network of users facing correlated, interdependent risks. Insurance is a powerful mechanism to promote network-wide changes, i.e lead to self protection. How to estimate damage? This is very hard on the internet. This paper shows how it is economical rational for entities to prefer a relatively insecure system to a more secure, and that the adoption of security investments follows treshold/tipping point dynamics. And that insurance is a powerful incentive to push the users over the treshold.

6.3 Modeling cyber-insurance: towards a unifying Framework

proposes a framework to classify models of cyber-insurance. Uses a common terminology, and deals with cyber-risk in a unified way.(combines the three risk properties, interdepenedent security , correlated risk, information asymmetri.) The paper studies other existing models, and reveals a discrepancy(AVIK) between informal arguments in favor of cyber-insurance and analytical results questioning the viability of a cyber-insurance market. Cyberinsurance, the transfer of financial risk associated with network and computers incidents to a third party, has been researched for several years. But reality continues to disappoint. Sets back by physical accidents such as 9/11 Y2K etc. Clients are for the most SMBs, limited market. Conservative forecast predicted cyber-insurance worth $2.5 billion in 2005. Jonas found a paper from 2012 that said the market was $800million.

All three obstacles has to be overcomed at the same time to fix the market, to do this we need a comprehensiv framework for modelling cyber-risk and cyber-insurance. many researchers have lost their optimism about cyberinsurance, but

this paper has not. Goal is that this unifying framework will help navigating the literature and stimulates research that results in a more formal basis for policy recommendations involving cyber-risk reallocation. Framework can also be used to standardize tcyber-insurance papers.

Breaks the modeling down to five key components:
- network environment(nodes controlled by agents, who extract utility. The risk comes from here
- demand side(agents)
- supply side(insurers)
- information structure, distribution of knowledge among the players.
- organizational environment. public and private entities whose actions affect netwrok security and agents security decisions.

what can be answered with models of cyber insurance markets?

1. Breadth of the market:Looking at equilibrium we can determine under which conditions will a market for cyber-insurance thrive? or what are the reasons for failure, and how can we overcome this?
2. Network security: What is the effect of an insurance market on aggregate nework security? Will the internet become more secure?
3. Social welfare: What are the contributions to social welfare?

6.3.1 Network Environment: Connected nodes

Two properties distinguish cyber-insurance from regular insurance.

1. Interconnected devices in a network, this generates value, therefore risk and loss analysis must take this into account.
2. Dual nature. if operational: generate value, else loss sources. When abused generate threat to other nodes.

network is not necessarily a physical connection, also includes logical link or ties in social networks.

Defense function Defense function D describes how security investment affects the probability of loss p and the size of the loss l for individual nodes. In most general its a probability distribution. An agent i only chooses s_i and takes the the vector of all other nodes level of security as given. This is how we model interdependent security.

network topology G Describes the relation between elements of an ordered set of nodes.(connectivity)

- star-shaped
- tree shaped
- ER
- Structured clusters

There are no literature using scale-free graphs, even this topology is a good fit with real world networks. Network topology shapes the risk arrival process, or defines the information structure when asymmetric information is considered.

Layers of multiple topologies for different properties of cyber-risk ar conceivable, i.e to model the specific influence of social and physical connections. But this will complicate the model.

Risk arrival defined by the relation between network topology G and the value of the defense function D Two cases:

1. no risk propagation, easy to tract analytically.
2. risk propagation, this is harder, need recursive methods or approximations, and may lead to a dynamic equilibria. both interdependent and correlated risk is modelled.

Cyber risk is characterized by both interdependent security and correlated risk, which both have a common root cause: interconnected nodes. Interdependent risk is usually modeled on the demand side, in contrast correlated risk is just a supply-side problem.

Attacker model existing literature assume attacks are perfomed by "nature" rather than strategic players. But attackers react to agents and insurers decisions. this paper models attackers as players. but it might be hard to choose reasonable assumptions and parameters for their capability. They could be modeled as an additional class of players or a special type of agents.

6.3.2 Demand side agents

Make security decisions for one or more nodes. When buying full coverage of risks, permits the agent to exchange uncertain future costs with a predictable premium.

Node control Agents have node control, mapping one to one, or one to many. Agents choose security investments for the nodes.

Heterogenity Agents(and associated nodes) are either heterogen or homogeneous in:

- their size of the loss
- their wealth
- their defense function
- their risk aversion and this utility function.

agents are homogenous if all of the above statements are identical for them.

Risk Aversion They only seek insurance if they are risk averse(accept lower expected income if they can reduce uncertainty).

Action space Established models differ in the action space for agents purchasing insurance. Options are:

Full or partial. Full, the only choice is between full coverage of the potenital loss or no insurance at all, i.e. binary choice. A contract is called fair if the expected profit from it is zero(insurers point of view). If premiums are actuarially fair, risk averse agents strictly prefer full over partial coverage. If premium is above fair lvl, partial insurance are demanded.

Security investment: agents can self-protect by choosing $s_i > 0$, which result in less expected loss. Selfprotection creates an externality, ie interdependent security. Second kind of security investment, i.e selfinsurance, this does not generate externality, it only reduces your own size of potential loss.

Enogenous network formation: changes to the network topology as operable actions for agents is not yet explored by literature. For example, agents ccould destroy/create links to other nodes with the goal of reduce their expected loss. A simple first step would be to consider platform diversity and switching(f.eks mellom OS) as an endogenous network formation problem.

Time Simple models, single shot. i.e all choices are set only once by all agents(not necessarily at the same time.) This may not be enough when risk propagation is present. To avoid ambiguity the order should be specified in the model formulation, f.eks from the center of a star-shaped to its leaves.

6.3.3 Supply side, insurers

Modeling decisions: monopoly, oligopoly or competition? Homogenous or heterogenous? The dominant model used in literature is naive, homogenous and competitive insurer market. It is important to include these as players. Five attributes: market structure, risk aversion, markup, contract design and higherorder risk transfer.

Marketstructure , monopoly, oligopoly or competition. Homegenous or heterogenous? Competitions leads to low MC.

Risk aversion A simplification in economic textbooks is to use risk neutral insurers. But to avoid taking excessive risk and bankruptcy due to profit maximization, need a safety capital. Regulators decide a maximum residual risk.

Markup : insurers profit, admin-costs, cost of safety capital.

Contract design : fixed premium, premium differentiation, contract with fines.

Higher order risk transfer : Insurers need not be the last step in a chain of risk transfer.

Cyber-reinsurance, the usual way to do this is by generating pools of loosely correlated risks, i.e the loss events from the tail of the probability distribution. This is usually done by creating a pool from regional or international diversification. Cyber-reinsurance is virtually not existent, due to the global homogeneity of cyber risk.

catastrophe bonds, financial instrument which pay a decent yield as a risk premium in periods without catstrophic events, but lose their value when such an event occurs. These are inadequate for cyber-risk, because thei may generate an incentive for investors, to cause a cyber attack.

exploit derivatives. Links payout of financial instrument to the discovery of vulnerabilities in systems. This is better than cat-bonds.

6.3.4 Information structure

Symmetric and asymmetric. Leads to adverse selection if the insurer cant distinguish between the agents. Moral hazzard occurs if agents could undertake actions that affect the probability of loss ex post. Also information about security is hard to gather and evaluate,. . All this results in two types of contract scenario, pooling or separation(agents sort them self out).

- adverse selection, if the insurer cant distinguish agents before signing contract.
- moral hazzard, if agents can undertake actions that affect the probability of loss after signed contract. i.e. not locking the door.

From classical economics, insurers have to ways of creating the contract when they cannot distinguish the agents, pooling or seperating(agents sort them self out). there is practically understood and observable that strong disincentives keep information sharing below socially optiimal levels. Relevant information may not exist, but it is often the case that it exists but is not available to the decision maker.

6.3.5 Organizational Enviroment(stakeholders)

four relevant attributes: regulator, ICT manufacturers, network intermediaries and security service providers. How to include these into models of cyber-insurance markets?

Regulator Government/governmental authority, with power to impose regulation. Important for policy analysis.

- disclosure requirements, can improve information for agents and insurers.
- Taxes, fines and subsidies to alter agents and insurers cots.
- Mandatory security impositions.
- prudential supervision, the regulator defines the acceptable residual risk, the probability of insurer bankruptcy.

ICT manufacturers vendors of hardware and software equipment.

- system security: ICT manufacturers prioritization of security affects the defence function of nodes using their products.
- System diversity, market structure affects correlation in the risk arrival process.

Network intermediaries Provide network connectivity services, ISP, registrars, and application service providers. they can contribute to distributed defense by sharing info about threats or taking down compromised nodes, reducing risk propagation. They can also shape the network topology, generating a more safe topology. Problems: different incentives for different ISPs, such as large versus small ISP.

security service providers Contribute to network security, in helping to overcome information asymmetries through collection and aggregation of information as a trusted third party, or improve information efficiency in monitoring and enforcing contracts. (Forensic investigations certifying etc.)

6.3.6 Using this framework for a literature survey

This framework accounts for three factors, correlated risks, interdependent security and information asymmetries.

demand side some papers have homogenous agents, others have heterogenous. Contracts with deductibles are standard tools to deal with information asymmetries. These are introduced in 4 papers. All models featuring interdependent security must allow for some kind of security investment via self-protection(binary or continous choice). Partial insurance is common, or full for simplicity.

Supply side Homogenoues and perfectly competitive insurers, and premium markups. Several authors interpret the markup as a reflection of market power.

Organizational Environment Current formal models are not good at capturing parameters of the organizational environment. Do insurance need to be mandatory, or will a simple punnishing of agents underinvesting in self-protection be sufficient. Rebates and fines are also discussed in one paper.

Research Question No paper who capture all three obstacles theoretically and link them with social welfare. Only one study evaluates its model from the perspective of all three research questions: breadth of the market, network security, and social welfare. Literature inspured by interdependent security primarily investigates network security, the most natural variable of interest in this setting. By contrast, Correlated risk and information asymmetries are studied from the point of vie of explaining a missing market.

Discussion of models The results from the papers are very dissappointing, so one may ask what are they good for. They give intuition on specific aspects and help generate a general view.

Despite early optimism about positve effects of cyber-insurance on network security, the existing models find that insurance markets might fail. And if a market exists, it tends to have adverse effects on incentives to improve security. Future research: endogenize parameters that are exogenously given in the existing literature, information structure and or organizational environment. for instance network topology.(This is what we will try to grasp, let the topology be generated

endogenizely. final observation: researchers write about how insurers will improve infomartion about security, but does not give any examples that reflects this. Affect agents choices of network products, but existing models of contracts do not reflect these choices. aggregate info about security(obtained from claims), but they do not model it parametrically. etc.....

6.4 A novel cyber-insurance Model

eliminate threats which cannot be tackled through traditional means, such as AV. Risks arrise due to both security attacks and non-security related failures. This paper analyzes cyber-insurance solutions when a user faces risks due to both of these. Propose a model called "Aegis", user accepts a fraction of loss recovery and transfers the rest.Mathematically show that only under conditoons when buying cyber-insurance is mandatory.

6.5 A solution to the information Asymmetry Problem

AV and other security software reduces the risk, but does not remove it completely. Cyber-insurance, residueal risk elimination. But a problem with this is information asymmetry. This paper proposes three mechanisms to resolve this problem. Mechanisms based on the principal agent problem, difficulties in motivating one party(the agent) to act in the best interests of another (the principal) rather than in his or her own interests. Arises in almost every case where a party pays another party to do something. The agent has more information than the principal, asymmetric.

1 cyber insurance who only provide partial coverage to the insureds will ensure greater self defense efforts.

2 the lvl of deductible per network user contract increases in a concave manner with the topological degree of the user.

3 Cyber-insurance market can be made to exist in the presence of monopolistic insurers.

Security experts claim that it is impossible to achieve perfect internet security just via technological advancements.

1 there do not always exist fool-proof ways to detect and identify. Even the best software available have false-positive, false-negative. And threats evolve automatically in response to AV-software being deployed.

2 The internet is a distributed system, different security interests and incentives pr user. Might spend money to protect their own hard drive, but not on prevent its computer being used by an attacker for a DOS attack on a wealthy corporation.

3 Correlated and interdependent risks. As a result, a user who invest in security generates positive externality for others. Which will result in a free rider problem.

4 Network externalities due to lock-in and first mover effects of security software vendors affect the adoption of more advanced technology.

5 Security software suffer from lemons market.

Cyber-insurance and asymmetry insurers are inable to disttinguish high and low risk users, i.e adverse selection. users undertaking actions, i.e moral hazard.

Difficult for insurers to gather information about applications, software installed, security habbits etc. and users can hide inforamtion.

Users in general invest to little in self-defense relative to the socially efficient lvl due to the free-rider problem(externatlities). Thus the challenge to improving overall network security lies in incentivizing end users to invest in sufficient amount of self defense.

6.6 Cyber-insurance for cyber-security, A topological Take on Modulating Insurance Premiums

Adopts a topological perspective in proposing a mechanism that accounts for the positive externalities, network location of users, and provide appropriate way to proportionally allocate fines/rebates on user premiums. Uses GT to prove. Consider a monopolistic cyber-insurer, prodividing full coverage. Each client is risk averse. A users investment and location in network determines his risk type. Each user has a utility function dependent on the rest of the users. Node centrality, maps to the externality effects a node has on other network nodes. Uses eigenvectors and bonacich papers. both these assign relative importance scores to all nodes, based on the concept of connections.

6.7 Differentiating Cyber-insurance Contracts, a topological Perspective

Important to discriminate network users on insurance contracts. prevent adverse selection, partly inernalizing the negative externalities of interdependent security,

achieving maximum social welfare , helping a risk-averse insurer to distribute costs of holding safety capital among its clients, and insurers sustaining a fixed amount of profit per contract. Important to find a way to properly discriminate. The paper propose a technique based on the topological location of users that allows cyber-insurers to appropriately contract discrimanate their clients. Consider single cyber-insurer providing full or partial coverage. Insurer have complete information about the topology. Discriminates on Bonacich/eigenvector centralities.

Chapter 7
Network formation: stability and efficiency

7.1 Survey of models of network formation: stability and efficiency

There is lots of economic situation where network structure plays an important role. It is very important to have information on how these structures form and matter. We can divide networks into two kinds, the ones where one central agent structures the whole network, such as airline network, or networks who are formed out of many different individuals decisions. This survey is about the second case, network connect a number of individuals.[Jac05] Three questions to focus on:

- How are such network relationships important in determining the outcome of economic interaction?
- How can we predict which networks are likely to form when individuals have the discretion to choose their connections?
- How efficient are the networks that form and how does that depend on the way that the value of a network is allocated among the individuals?

7.1.1 Defining Network Games

Players $N = 1, ...n$ set of players or individuals(organizations, firms, people, etc), modeled as nodes.

networks May take many forms, non-directed, directed networks. A network g is a list of which pairs of players are linked to each other. $N(g)$ is the set of players who have at least one link in the network g.

Paths and components Components of a network are the distinct connected subgraphs of a network, components of g are denoted $C(g)$.

Value functions

Network games

Allocation rules to know how much the total value of the network, we need to know how the value is allocated or distributed among players.

Chapter 8
Related work 2

Virus and worm propagation on the Internet can be modeled as epidemic spreads. When we look a 2-agent model we can observe correlation between one agents choice of investing in protection. If agent 1 has a connection to agent 2, the probability of agent 2 being contagion is strongly correlated to the choice of agent 1. In the case where agent 1 invests in protection, agent 2 will not be infected. However, if chooses not to invest in protection, the probability of infection for agent 2 is p. After a number of equations the authors conclude that in presence of insurance, the optimal strategy for all users is to invest in self-protecting services as long as this cost is low enough.

Further the authors looks at the situation where the cost of selv-protection is different for different agents (heterogeneous users) in a complete graph (n-n). The conclusion states that insurance increase the adoption for a fraction of the users, which creates the cascading effect that the rest of the users also gains benefit from investing in insurance. We end up in a state where everyone in the network are self-protected.

In star shaped graphs (i.e. hubs), it is obvious that the network will decrease the probability contagion dramatically by investing in self-protection measures. The authors also assumes that it is likely that the other low connectivity nodes will follow the hub and adopt self-protection.

Chapter 9
Network Games

In the paper [Blu11], they come up with some interesting results regarding network formation games. They set up a game where the nodes benefit from direct links, but these links also expose them for risk. Each node gains a payoff of a per link it establishes, but it can establish a maximum of δ links. A failure occur at a node with probability q, and propagates on a link with probability p. If a nodes fail, it will receive a negative payoff of b, no matter how many links it has established.

The results from their model shows a situation where clustered graphs achieve a higher payoff when connected to trusted agents, compared to when connecting with random nodes. Unlike in anonymous graphs, where nodes connect to each other at random, nodes in these graphs share some information with their neighbours, which is used when deciding whether to form a link or not. To further explain these results, they show that there exists a critical point, called phase transition, which occurs when nodes have a node degree of $1/p$. At this point a node gets a payoff of a/p, to further increase the payoff the node needs to go into a region with significantly higher failure probability. Because once each node establish more than $1/p$ links, the edges which propagates risk, will with high probability form a large cluster. Which results in a rise in probability of node failure, and reduces the overall wellfare. From this the paper say that when the minimum welfare exceeds $(1 + f(\delta) * a/p)$ we have reached super critical payoff. Otherwise it is called sub-critical payoff. Further they show that the only possible way of ending up with supercritical payoff, is by forming clustered networks consisting of cliques with slightly more than $1/p$ nodes. If the nodes form an anonymous market, random linking, they can only get sub-critical payoff. In other words, if the nodes can choose who they connect with, and by doing so, creating trusted clustered markets, they can achieve a higher payoff, by exceeding the critical node degree point. But in random graphs, this is not possible.
notater The paper [Blu11] describes a model which seeks to capture the underlying trade-off between the benefits of adding new links and the problem with increased contagious risk. Results from the model describes a situation where clustered graphs

achieve a higher payoff when connected to trusted agents. This phenomena is called super-critical payoffs. Unlike in anonymous graphs, which are completely random, nodes in these graphs share some information with their neighbors, which is used when deciding whether to connect or not. The cliques, forms a clustered network of agents which trust each other, consequently the risk of cascading failures are lower. Inspired by this model, we created a model which shields light on how cyber-insurance can be used in network formation to prevent cascading failures and increase an agents payoff.

notater„, The notion of stable, is a relaxation of pairwise nash-stability, and is defined as:

- no node can improve their payoff by deleting all its links(removing itself from the network)
- There is no pair of nodes, i, j, who are not a part of the network G, who would have gained a higher payoff by joining the network.

This paper[GGJ+10] provide a framework for analyzing situations when a players actions is influenced by neghbourhood structure, modeled in terms of an underlying netwrok of connections that affect payoff. The players are partially informed about the structure.

There are many social and economic interactions where an agents well being depends on her own actions as well as on actions taken by others, i.e. externalities.

References

[Ake97] George A Akerlof. The market for" lemons": Quality uncertainty and the market mechanism. *Readings in Microeconomic Theory*, page 285, 1997.

[And10] R.J. Anderson. *Security Engineering: A guide to building dependable distributed systems*. Wiley, 2010.

[Aud] Jan A. Audestand. Some aspects concerning the vulnearbility of the computerized society. http://www.item.ntnu.no/_media/academics/courses/ttm6/vulnerability.pdf. Accessed: 20/02/2013.

[BL08] Jean Bolot and Marc Lelarge. Cyber insurance as an incentive for internet security. *Managing information risk and the economics of security*, pages 269–290, 2008.

[Blu11] Easley D. Kleinber J. Kleinberg R. anad Tardon E. Blumen, L. Network formation in the presence of contagious risk. 2011.

[BMR09] T. Bandyopadhyay, V.S. Mookerjee, and R.C. Rao. Why it managers don't go for cyber-insurance products. *Communications of the ACM*, 52(11):68–73, 2009.

[Böh10] Rainer Böhme. Towards insurable network architectures. *Information Technology*, 2010, 2010.

[Bol85] B. Bollobás. Random graphs. *Academic Press*, 1985.

[Bro] RTM Insurance Brokers. Rtm's hackersforsikring. http://www.hackerforsikring.dk/index.html. Accessed: 13/02/2013.

[BS10] R. Böhme and G. Schwartz. Modeling cyber-insurance: Towards a unifying framework. *Proceedings of GameSec*, 2010, 2010.

[CfAPA] CAPA Centre for Asia Pacific Aviation. Skywest airlines. http://centreforaviation.com/profiles/airlines/skywest-airlines-oo. Accessed: 08/04/2013.

[CoA] Travelers Casualty and Surety Company of America. Cyberrisk. https://www.travelers.com/business-insurance/management-professional-liability/Cyber-Risk.aspx. Accessed: 31/01/2013.

[dig] digi.no. Vil forsikre alt og alle på nett. http://www.digi.no/39107/vil-forsikre-alt-og-alle-paa-nett. Accessed: 18/02/2013.

[EK12] D. Easley and J. Kleinberg. Networks, crowds, and markets: Reasoning about a highly connected world, 2012.

[Faa] faa Federal aviation administration. Calendar year 2011 primary airports. http://www.faa.gov/airports/planning_capacity/passenger_allcargo_stats/passenger/media/cy11_primary_enplanements.pdf. Accessed: 08/04/2013.

[Gar07] Argyrakis P. Garas, A. Correlation study of the athens stock exchange. 2007.

[GGJ+10] A. Galeotti, S. Goyal, M.O. Jackson, F. Vega-Redondo, and L. Yariv. Network games. *The review of economic studies*, 77(1):218–244, 2010.

[Ins11] Ponemon Institute. Second annual cost of cyber crime study, benchmark study of u.s: Companies. Technical report, Ponemon Institute, Aug 2011.

[it] Dagens it. Forsikring mot hackere. http://www.dagensit.no/arkiv/article1345297.ece. Accessed: 14/02/2013.

[Jac05] M.O. Jackson. A survey of network formation models: Stability and efficiency. *Group Formation in Economics: Networks, Clubs and Coalitions, ed. G. Demange and M. Wooders*, pages 11–57, 2005.

[LHN05] Erez Lieberman, Christoph Hauert, and Martin A Nowak. Evolutionary dynamics on graphs. *Nature*, 433(7023):312–316, 2005.

[MCR80] R.I. Mehr, E. Cammack, and T. Rose. *Principles of insurance*. RD Irwin, 1980.

[New] Graeme Newman. Cyber liability in europe: What insurers should knowl. http://www.cfcunderwriting.com/media/news-articles/european-cyber.aspx. Accessed: 14/02/2013.

[Nor] Gjensidige Nor. Medlemsfordeler hos gjensidige 2012 - nal. http://www.arkitektur.no/gjensidige?iid=372345&pid=NAL-Article-Files.Native-InnerFile-File. Accessed: 14/02/2013.

[Pal12] Ranjan Pal. Cyber-insurance for cyber-security a solution to the information asymmetry problem. May 2012.

[PD12] National Protection and Programs Directorate. Cybersecurity insurance workshop readout report. *U.S. Department of Homeland Security*, 2012.

[PpD12] National Protection and U.S. Department of Homeland Security programs Directorate. Cybersecurity insurance workshop readout report, Nov 2012.

[Pra] Mary K. Pratt. Cyber insurance offers it peace of mind – or maybe not. http://www.computerworld.com/s/article/9223366/Cyber_insurance_offers_IT_peace_of_mind_or_maybe_not?taxonomyId=17&pageNumber=1. Accessed: 31/01/2013.

[Ris12] Stratic Risk. Evolving cyber cover. http://www.strategic-risk.eu/Journals/2012/02/22/i/j/w/RiskFinancing_Mar12.pdf, March 2012. Accessed: 31/01/2013.

[Rob12] N. Robinson. Incentives and barriers of the cyber insurance market in europe. 2012.

[Spa] Sparebank1. Spar inntil 25 https://www2.sparebank1.no/sr-bank/forsikring/skadeforsikring/fa-rabatt-pa-forsikringer/. Accessed: 09/04/2013.

[Wat11] Tower Watson. Despinte increasing cyber threats, most companies are not buying network liability policies. http://www.towerswatson.com/press/4482, May 2011. Accessed: 31/01/2013.

[Wik] Wikipedia. The market for lemons. http://en.wikipedia.org/wiki/The_Market_for_Lemons. Accessed: 13/02/2013.