NTNU – Trondheim
Norwegian University of
Science and Technology

Cyber Insurance

Håvard Halse
Jonas Hoemsnes

Submission date: March 2013
Responsible professor: Jan A. Audestad, Affiliation
Supervisor: Gergely Biczók, Affiliation

Norwegian University of Science and Technology
Department of Telematics

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

Skriv om virus og slikt generelt, mye angrep osv....

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. However, the concept of cyber-insurance has been around since the 1980s, but so far it has failed to reach its promising potential.

Cyber-insurance works the same way as traditional insurance, where the insurance contract (policy) binds the insurance company to pay a specified amount to the insurance holder when 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 will mean that the security is negatively correlated with the premium costs.

1.1 The basics of insurability

Generally, insurable risks possesses seven common 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 Three main obstacles

Cyber-insurance fit relatively well to the general insurance model, but 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 party 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, 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 buys insurance, but 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 is 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 similar. [Pal12]

As we will see the information asymmetry problem is highly relevant regarding cyber insurance. The measuring of security is very hard to perform, and thus people have a high incentive for hiding information about their security strength. Another problem arising due to information asymmetry, is the so called lemons market. It is difficult for a security software buyer to distinguish the performance(bad vs good) of different software, 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 between good and bad software. If the cost of producing good security software is to high, this problem can even result in the good ones chooses not to produce, because it would not be profitable.

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

Correlated risk Another big concern regarding cyber-insurance, is the correlated risk. In networks and computers standardization is very important, 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. The standards are what makes the ICT-industry valuable, but also what makes all the threats we are facing each day possible. 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. 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 uneconomical supply of cyber insurance. 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. bankruptcy.[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 the security the rest invest in. 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, it is dependent on the number of compromised computers, so even if you have invested in security software of some kind, you still receive lots of spam due to the fact that there are so many who has not invested. [Böh10]

Another concern regarding cyber-insurance is to the determine the value of the loss. 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 and 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, and the second one is probably the most difficult. Because it is not easy to set a value on the loss of secondary losses, i.e. how many potential customers did they loose due to the reputation loss, how many customers churned, and what was their value etc.

1.2.1 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 managment on the internet has involved 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. But unfortunately this does not eliminate the risks completely, threats evolve over time, and there will always be accidents. How can we handle this residual risk, this is where Cyber-insurance comes to mind, option 4, transfer the risk to a party who willingly accept it in exchange for a fee. This is the idea behind insurance in general, exchange costs of uncertain events with predictable periodical payouts, premiums. [BL08]

... Random notater: Although there are some problem areas, such as defining loss, where it often is difficult to demonstrate the location and cause of data breaches. Cyber-insurance appears to fit in to the general model of insurance. Standardization is important for network and computers, leading to many users using the same operation systems, and other software and hardware products, hence there is a large number of similar exposure units. Power outage, DoS-attacks etc. are usually a result of accidental loss.
Further, the premiums can be priced at a affordable level, in cyber-insurance the premium level will be highly dependent upon the companies security systems and policy. This also relates to the calculable loss, where better security systems yields lower probability for incidents. [Rob12] Another problem cyber-insurance has to face is the fact that losses might be correlated, resulting in insurance companies have to pay large numbers of claims at once. Examples are policies including insurance against lost income due to denial of service of websites. 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.

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 due to the fact that insurance companies only will indemnify the losses where victim can prove that a certain event has occurred. When it comes to cyber insurance, one often need computer forensics to generate the evidence needed.

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 attracting 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

3.1 Graphs

Most activities in nature and society can be described using graphs, which offers an intuitive approach that can be analyzed. Railroads, water pipelines, societal relations etc. can all be described using graph theory. In addition, the Internet and other computer networks is formed and evolves according to the laws of random graphs [Aud]. Graphs serves as an analytic tool [Aud], which in our case makes it possible to investigate whether there are certain graphs that might yield higher security than others. This section will provide background information on how these graphs are created, and highlight the main characteristics which are important for detecting insurable topologies.

3.1.1 Basic graphs

There are some basic properties of graphs which is important to be familiar with. Figure 3.1 depicts the basics of an unweighted graph, meaning the edges are not given any value. In other cases, weighted edges is useful to e.g. reflect capacity constraints such as a link's maximum bandwidth. Other common definition used in the description graphs are described below [Aud]:

- Edge degree: Number for edges connected with a vertex.
- Hub: Vertex with high edge degree.
- Cycle: A chain originating and terminating at the same vertex.
- Cluster: Subgraph of highly connected vertices.
- Cluster coefficient: Probability that two vertices that are adjacent to a third vertex are also adjacent.
- Clique: Subgraph where all vertices 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 3.1.2).

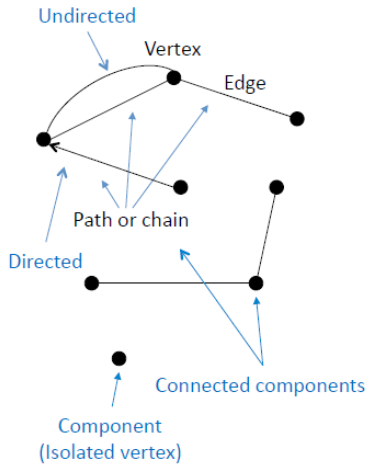


Figure 3.1: General graph [Aud].

3.1.2 Random Graphs

Regarding cyber-insurance the study of random graphs are of special concern, since we are looking for insurable topologies in computer networks(random graphs). The research on random graphs are fairly new compared with 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 over a fixed number n of vertices, where each node connects to another of the $n-1$ vertices with a chosen probability p. The resulting graph will on average contain $n(n-1)p/2 \approx n^2p/2$ edges [Bol85]. From analyzing the graph, the authors found some interesting properties[Bol85][Aud]:

– 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.

Our goal is to use a graph which models how to Internet and other computer networks are connected. A fully connected E-R graph has a good potential, since the graph will have a short diameter similar to the Internet. However, the edge degree follows a Poisson distribution, which means that the edge degree 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.

Albert-Barabási Graphs

The struckture which is believed to be most accurate regarding modeling the structure of 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 a vertex have a very high edge degree.

A-B graphs can grow and become scale-free if every new vertex is connected to one or more existing vertices with a probability proportional to the edge degree of these vertices [Aud]. The paper [Aud] presents an algorithm creating A-B graphs and figure 3.2 models a possible formation of a graph using the 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, and the graph does not contain loops.

In addition to the high clustering coefficient the research found that these graphs have a fairly small diameter, which is noticeable from the graph depicted above. A-B graphs are therefore comparable to the network formation of the Internet and other

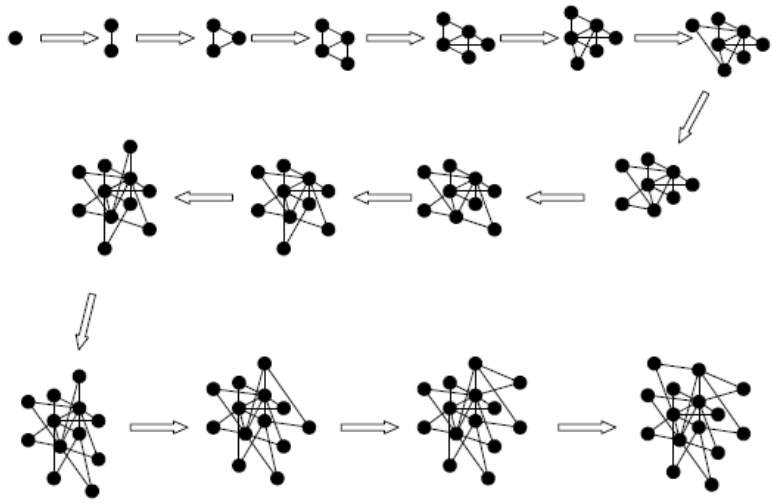


Figure 3.2: Forming a A-B graph in 15 generations [Aud].

computer networks. The model is therefore a good base in the search for insurable topologies.

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

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, since risks are correlated, one problem is for the insurer to be able to calculate the overall probability of casualty/infection. The paper [LHN05] is about evolutionary dynamics and how certain structures can amplify or sustain evolution or drift. This is very usefull for our study of insurable topology, if one can determine some structures, where certain nodes have certain properties, and these structures then will sustain viruses from spreading, or amplify the incentive for obtaining cyberinsurance and antivirus, then we can possibly determine if it is an insurable topology.

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

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

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.

The important question that this paper answer, is if it is possible to find graphs with fixation probability that exceeds 4.1?, and if so, is it possible to suppress drift and amplify selection or visa versa?

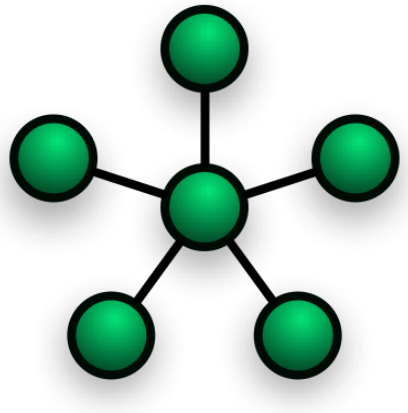


Figure 4.1: A star-topology [LHN05].

The paper shows that in certain graphs this is possible, one example is the star topology 4.1. In this topology the fixation probability is

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

. or more generally:

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

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

When applying this to our scenario, cyber insurance and insurable topologies, we can use this to show that if the center node is strongly secured, then the virus will be considered as disadvantageous and it will be inhibited from fixation with a certain probability. This makes the overall risk easier to calculate for both the insurer and the nodes, and makes it possible and easier to calculate fair and affordable premiums. It can also be used as an incentive for the center node to buy insurance or security software, because it can easily be shown how probable an infection will occur.

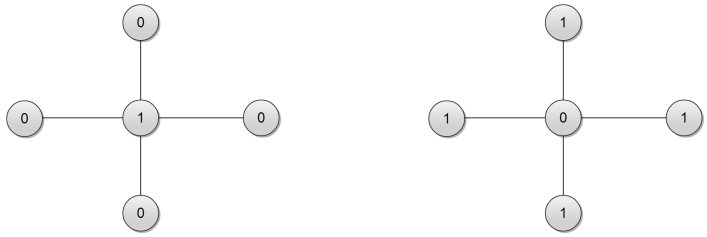
One could for example force the center node to buy sufficient anti virus, by informing it about how likely it will be infected, and how expensive the cyber insurance will be if it do not invest sufficiently in self protection. This will make the whole network more secure, and the insurer can now offer insurance to the leaf nodes for a fair price with a calculable risk. This could also be used to show how

information about cyber-insurance or protection software will spread throughout a network, and if the information is advantageous, eventually all nodes will acquire the insurance or software.

There are other graphs where the fixation probability is equal to 4.3, funnel and metafunnel. And as we know from the (Kapittel om scale-free and naturlige nettverk) there are many toplogies in our society that are similar to these graphs. In all of these, it can be shown that if N is large enough, the fixation probability for advantageous mutant converges to 1, and for disadvantageous converges to 0.

4.0.3 Network games

In the paper [GGJ+10] they show how network games evolve when the payoffs are determined not only by your own decisions, but also by your neighbours. A game that is applicable to our scenario is when considering security software, security software can be considered as a public good, it suffers from strategic substitutes, i.e. that if your neighbour acquire it, it gives you less incentive to also acquiring the software. Public goods and security also benefits from positive externalities, when one acquires the software, all the neighbours benefits from it, because the risk of being infected decreases. 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 of the game is 1 if $y_i >= 1$ and 0 otherwise. There is a cost of choosing the action 1, and the cost is: $0 < c < 1$.



(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.

When we look at the star example, we easily see that there is two equilibriums

4.2, one 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: $\#leafnodes * c$ versus the first equilibrium where the total cost is only c. If we could have forced to network game to end up in the socially optimal equilibrium, this would have been optimal. One possibility could be for the insurer to offer cheap insurance to all the leaf nodes, and a expensive one to the center node. By expensive we mean a cost that exceeds the cost of acquiring self protection, because then a rational center node would striclty prefer buying security software, as long as the price for acquiring and maintaining it is less than the possible cost of loss.

$$U_{center} = -Probability_{casualty} * \alpha - Cost_{selfprotection} \tag{4.4}$$

A risk averse player would like to maximize her expected utility 4.4. We assume that the probability of casualty is significantly smaller when acquiring self protection, versus not acquiring. If the options for a player is either to remove the expected loss of casualty by acquiring self protection, or by insuring against it, and the expected utility of acquiring insurance is lower than the expected utility of acquiring self protection. The player would strictly prefer self protection. This is one possible way of forcing the network game to end up in an insurable star topology. // Thoughts on what this fixes in a simple way... The insurer can now calculate the probability for catastrophic event(all nodes suffer), and now atleast has a measurement on the correlated risk. It has also limited the information asymmetry to concern only one node, the center node. It does not matter if the leaf nodes acquire security or not. Also it has now limited the interdependent security to one node, the center node.

// // notater:

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

	A	B
A	a	b
B	c	d

Table 4.1: Setup propagation game [LHN05]

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.

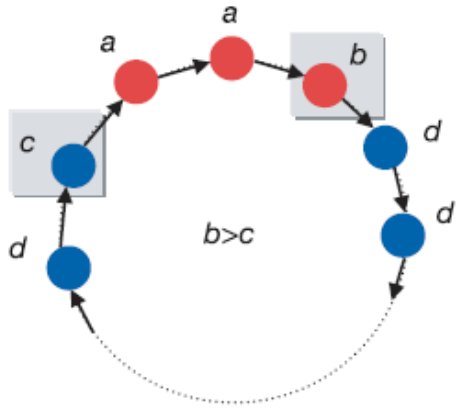


Figure 4.3: Mutant propagation game

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.

To be able to point out 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 fits in to the model of security.

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 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?

And the selective difference is as we see amplified from r to . i.e. a star act as an evolutionary amplifier, favoring advantageous mutants and inhibiting disadvantageous mutants, tilts towards selection and against drift.

in certain graphs, star, funnel, metafunnel, if N is large enough, fixation probability for advantageous mutant converges to 1. Fixprob for disadvantageous converges to 0.

The same theory can be used to demonstrate how the aggregated security of a network is higher if the central node of a star structure is secured. If we assume that implemented security is 100% efficient, no threats will propagate beyond that node i.e total security for the network is increased. Scale-free networks have most of their connectivity clustered in a few vertices, i.e. they are potent selection amplifiers.

Chapter 5
Relatedwork

5.1 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.

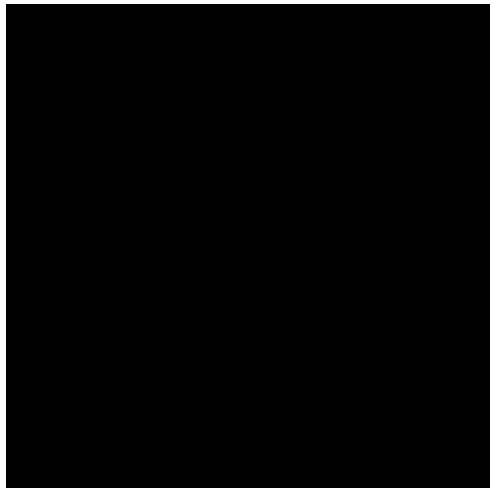


Figure 5.1: A figure

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.

5.2 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).

5.2.1 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.

5.2.2 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.

5.3 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?

5.3.1 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.

5.3.2 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.

5.3.3 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.

5.3.4 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.

5.3.5 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.)

5.3.6 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.....

5.4 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.

5.5 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.

5.6 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.

5.7 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 6

Network formation: stability and efficiency

6.1 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?

6.1.1 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 7
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 8
Network Games

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.

Chapter 9
Modeling Cyber-Insurance

9.1 Network Formation

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 a 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] 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.

9.1.1 Model of handling contagion risk

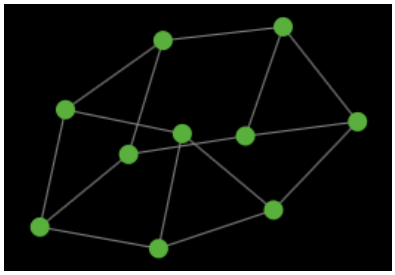
The model is simplified in order to show the concept of using cyber-insurance to encounter the problems with contagious risk. The model is formulated as follows. A set of n agents are randomly chosen to be insured or not. They all get their own income, and by connecting to other agents they will benefit from their income, i.e. when connected both agents will increase their income. However, when connecting to another agent naturally the cost of insurance increases due to aggregated risk. If and agent connects to someone without insurance a possible risk of severe losses due to cascading failure r has to be taken into account.

α - an agents income
β - income from direct links
I_o - cost of insurance.
I_l - increased insurance cost due to risk from a direct link.
r - cost of not having insurance, in case of failure.

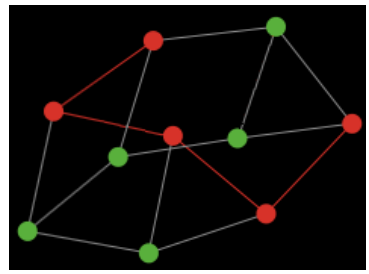
Each agents payoff π is calculated with the following equation.

$$\pi = \alpha + \beta - I_o - Il - r \tag{9.1}$$

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 9.1 clustered networks of insured agents (red) are created, and according to [Blu11] the these agents achieves super-critical payoffs. Which demonstrates that



(a) Initial graph with 10 agents.



(b) Insured agents (red) forms a network

Figure 9.1: shows how insured agents connects with each other to form a network to achieve super-critical payoffs.

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.

[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.

[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.

[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.