NTNU – Trondheim
Norwegian University of
Science and Technology

Cyber Insurance

Håvard Halse
Jonas Hoemsnes

Submission date: February 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

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.

«««< HEAD 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 more secure a company is, the lower the premium costs. ======= 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 more secure a company is, the lower the premium costs. »»»> aaad1a852a51fef71c67580bc15d26bf68446c92

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.

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. [BS10] 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.

Correlated risk ««««< HEAD Another big concern regarding cyber-insurance, is the correlated risk. In networks and computers standardization is very important, it enables computers to communicate, install software, the standards

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 company's 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 a large number 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. ======= Another big concern regarding cyber-insurance, is the correlated risk. In networks and computers standardization is very important, it enables computers to communicate, install software, the standards 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. »»»> aaad1a852a51fef71c67580bc15d26bf68446c92

... Random notater: 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.

Despite the widespread awareness of cyber crimes, cyber attacks occur frequently. The companies studied in [Ins11] experienced successfull 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 $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 offering cyber protection, but there are still many companies not utilizing them, in a survey of 13000 companies, 46 percent said they had a cyber insurance. [Pra]

Another paper [Ris12] collected statistics in the UK, which 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. 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 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]

We conducted a market survey of the Norwegian cyber insurance market. Compared to the US and UK market there are little information about it current state. In Norway there are few actors offering any kind of cyber-insurance, in addition they wasn't eager to share any information from their customer base. Therefore it was not possible to get any estimates on how big the current Norwegian market is. Despite today's low activity, the survey revealed that around year 2000 there was taken steps towards establishing a cyber-insurance market in Norway. Startup companies such as Safensure AS, dedicated to deliver cyber-insurance to the Norwegian and European market, and major insurance companies, such as Gjensidige Nor started offering insurance against loss income due to malicious hacker attacks, denial of service and other characteristics of cyber-insurance. 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 are taken by the company (REF: http://www.dagensit.no/arkiv/article1345297.ece). Today, the same company offers something they call operation-loss-insurance which covers expenses due to denial of service, software-insurance which covers expences regarding reconstruction of files and reinstalling software, it is also possible to insure against hacking and sabotage. 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. http://www.hackerforsikring.dk/index.html

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
Relatedwork

3.1 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.

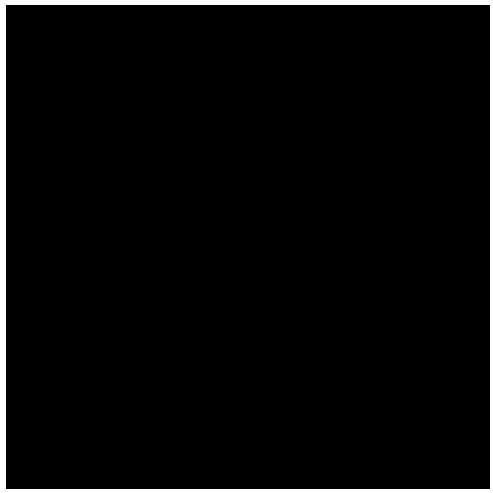

Figure 3.1: A figure

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.

3.2 Cyber insurance as an Incentive for Internet Security

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).

3.2.1 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.

3.2.2 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 benets 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.

3.3 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?

3.3.1 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.

3.3.2 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.

3.3.3 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.

3.3.4 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.

3.3.5 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.)

3.3.6 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.....

3.4 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.

3.5 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.

3.6 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.

3.7 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 4
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.

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.

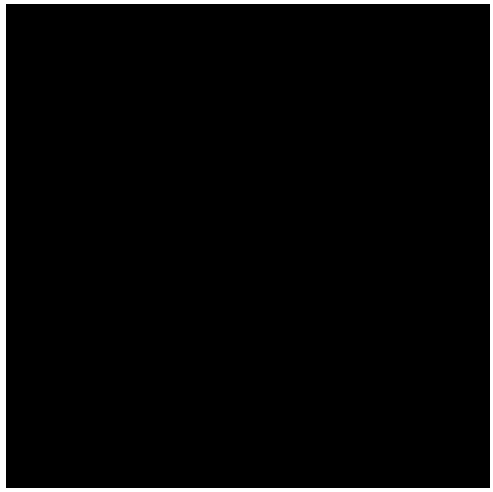

Figure 4.1: A figure

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.

Table 4.1: A table

a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	q	r	s	t
u	v	w	x	y
z	æ	ø	å	

4.1 First section

4.1.1 First subsection with some $\mathcal{M}ath$ symbol

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.

- item1
- item2
- ...

4.1.2 Mathematics

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. $\sin^2(\alpha) + \cos^2(\beta) = 1$. If you read this text, you will get no information $E = mc^2$. 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. $\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{ab}$. This text should contain all letters of the alphabet and it should be written in of the original language. $\frac{\sqrt[n]{a}}{\sqrt[n]{b}} = \sqrt[n]{\frac{a}{b}}$. There is no need for special content, but the length of words should match the language. $a\sqrt[n]{b} = \sqrt[n]{a^n b}$.

Proposition 4.1. *A proposition... (similar environments include: theorem, corrolary, conjecture, lemma)*

Proof. And its proof. □

4.1.3 Source code example

Algorithm 4.1 The Hello World! program in Java.

```
class HelloWorldApp {
  public static void main(String[] args) {
    //Display the string
    System.out.println("Hello World!");
  }
}
```

You can refer to figures using the predefined command like Figure 4.1, to pages like page 26, to tables like Table 4.1, to chapters like Chapter **??** and to sections like Section 4.1 and you may define similar commands to refer to proposition, algorithms etc.

References

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

[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.

[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.

[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.

[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.

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

[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.