BI Norwegian Business School - campus Oslo

GRA 19703

Master Thesis

Thesis Master of Science

Assessing Different Levels of Time Retention for Business Interruption Coverage on Cyber Insurance

Navn:	Mats Lambech, Kristoffer Sjur Høglo

Start:	15.01.2020 09.00
Finish:	01.09.2020 12.00

BI Norwegian Business School

Assessing Different Levels of Time Retention for Business Interruption Coverage on Cyber Insurance

Program:

Master of Science in Business, Major in Accounting and Business Control

Examination Code and Course Name:

GRA 19703 - Master Thesis

Supervisor:

Morten Lund

Hand-in Date:

29.06.2020

Acknowledgements

This master thesis is the culmination of our Master of Science program in Accounting and Business Control at BI Norwegian Business School.

We want to express our gratitude to our supervisor Morten Lund, for his guidance, advice, and help towards setting up interviews, without which this thesis would be limited to a far smaller scope.

We would also like to thank our interviewees Eirik Lund, Glennie Ingebrigtsen, and Nanna Unhammer, for their time, engagement, knowledge, and for helping us gain insight into their work and industry. Their cooperation was essential for this thesis.

Abstract

As a consequence of the digitalization in companies, cyber-related risk has increased substantially. Cyber insurance has, therefore, emerged as a tool to mitigate cyber risk. Cyber risk behaves differently compared to more traditional risks such as business interruption and property damage. These are relatively immobile, whereas cyber risk is fast-paced and has an inherent ability to simultaneously impact multiple entities, as well as having the potential to cause extensive damage in a short period of time, regardless of traditional limitations of risk such as geographical location and being contingent on tangible assets. Elements of traditional insurance policies, such as waiting periods and risk estimation, may thus be inadequately adapted to cyber risk.

This thesis, therefore, explores the effect time retention, i.e., waiting period, have on the expected utility of cyber insurance during a business interruption caused by a cyber incident. Through in-depth interviews with industry professionals, and analyzes of cyber policies, questionnaires, and underwriter guidelines, we developed a model which derived the expected utility of cyber-related business interruption coverage. The model was used to analyze and evaluate the current conditions of cyber-related business interruption.

The findings from the model illustrate that cyber-related business interruption coverage and current time retention levels for cyber insurance is neither well-adjusted nor suitable adapted to the present cyber risk exposure.

Table of Content

1 Introduction

1.1 Background for the Thesis

The complex and comprehensive nature of the modern business world triggers businesses' need to limit their scope of risks. For businesses, the need to mitigate the effect of business interruption due to cyber incidents are increasing. Thus, there is a need to observe how the prevailing conditions of business interruption coverage, fit in the modern world of business and cyber risk.

Technology is everywhere around us. We use our smartphones to check the weather and update us on the news. Cars can operate autonomously, and there are whole industrial complexes that are dependent on the Internet of Things (IoT), a method of communication between devices without humans intervening. This dependency on technology exposes companies to cyber risk, which involves the possibility of significant interruptions due to illicit actions, causing extensive implications for companies. As illustrated by McAfee and Center for Strategic and International Studies, the consequences can be colossal; having estimated the global cost of cybercrime to be as much as $600 billion in 2017 (CSIS & McAfee, 2018).

The increased interest in efforts to mitigate the impact of cyber incidents can be explained by cyber risk becoming increasingly relevant due to several cyber incidents across the globe. Cyber risk achieved heightened notoriety as a result of cyber attacks such as the NotPetya cyber attack in 2017 (Perlroth, Scott & Frenkel, 2017), the hack of Equifax, and the ransomware attack on Hydro in 2018 (Hydro, 2019). While also receiving public awareness, the attacks had a devastating economic effect on the affected companies. Among several companies that have experienced the impact of comprehensive attacks, Maersk, a shipping and logistic giant suffered losses between $250 million and $300 million from a cyber attack in 2017 (A.P.Møller - Mærsk, 2017, p. 54). Capital One, a financial corporation, had losses of between $100-150 million in 2019 due to a single cyber incident (Trefis Team, 2019). These incidents illustrate how comprehensive and damaging some of these attacks can be. The considerable worldwide technological advances are increasing companies' exposure to cyber risk. The question then becomes not who

is exposed to cyber risk, but how to effectively hedge this risk; one of these hedges may be what is known as cyber insurance.

As cyber risk has grown, the consensus has shifted from cyber risk being a concern only related to cyber security, but now also a concern for the business domain (Toregas & Zahn, 2014, p. 5). Cyber risk being a "business-problem" indicates that cyber security is no longer the only viable solution, but that business-related solutions such as insurance also can be used to mitigate some of the problems related to cyber risk.

The primary purpose of cyber insurance is to protect customers against uncertainty and loss, hence maximizing their profits through mitigation of their cyber risk (Kuru & Bayraktar, 2017, p. 3). Accenture Security, in collaboration with Ponemon Institute, identified that the average cost of cyber crime to "large-sized organizations" was $13.0 Million in 2018 (Accenture Security & Ponemon Institute, 2019, p. 11). The astounding costs of cyber crime and accelerating exposure due to technological progress have facilitated for the development of cyber insurance tools. The demand for cyber insurance is flourishing, as indicated by the NAICs report, which states an increase of 14.54% in the total U.S cyber insurance market from 2017 to 2018 (NAIC, 2019). While the demand is flourishing, the obstacle is estimating whether cyber insurance is economically sustainable to provide and to purchase.

Like any other insurance product, cyber insurance has its advantages and disadvantages. One of the current shortcomings of cyber insurance is the lack of empirical data and accurate estimation tools, which impedes the development of cyber insurance products. Lack of data, hereunder information on occurrences, and the comprehensiveness of the incidents reinforce the difficulty of estimating the relation between coverage vs. premium (Biener, Eling & Wirfs, 2015)**.** This shows that there is a substantial need for applicable economic hedges against cyber attacks. Therefore, it is important to research the potential impact and further implications of cyber insurance.

1.2 Purpose of the Thesis

Cyber risk can affect a company in several different domains; it being a ransomware attack, loss of intellectual property, or an incident that results in a business interruption and financial loss. Thus, risks may impact individual entities asymmetrical and be unique in duration and severity dependent on the circumstances of the risk and attributes of the entity. As a result, there is not a "one-size-fits-all". The proceeding conclusion is that entities may have a need for different design of policy when exposed to identical cyber risks. Therefore, the thesis aims to explore whether there is a positive return when given a choice of retention level in the form of an adjustable waiting period. This involves whether there exists an optimal level of time retention, given a probability and length of a cyber incident.

Toregas and Zahn (2014, p.5) state that the e-commerce market is worth $7 trillion, making it a lucrative target for cyber attacks. It was estimated potential losses of upwards to $3.4 million per hour during "cyber Monday" in 2013. Such losses can be detrimental to e-commerce businesses. Toregas and Zahn (2014, p.4) further state that the damage experienced by companies on average is more than $9 million. Which, in turn, promotes the necessity of a feasible economic hedge such as cyber-related business interruption coverage.

The demand for cyber-related business interruption coverage is soaring. Advisen and PartnerRe performed a survey in 2019 of insurance carriers and brokers as well as their customers, where they were given a choice of their top three most requested cyber coverage, concluding that business interruption was the top three choice of 61% of the respondents (PartnerRe & Advisen, 2019, p. 4). The complicated calculation of business interruption and the demand sides vague understanding of how the industry views the retention rates, these factors, combined with the poor fit of the waiting period to modern cyber risk, indicate that there is a significant potential for future research and exploration (Schumann, 2013; Cohen, n.d; Deloitte, 2016).

We want to observe and determine whether the current cyber insurance environment of business interruption coverage is suited for the comprehensive

nature of cyber risk. This is due to the unique properties of cyber incidents, such as the lack of geographical limitations, the scope of impact, and network effects enhancing the impact. This leads to the question of whether or not the current parameters for cyber-related business interruption coverage, are suited for companies exposed to cyber risk.

To estimate and analyze the effect the retention rates have on the expected utility of an entity, we will develop a model based on previous research on utility theory and insurance. Kuru and Bayraktar (2017) illustrated a simple function for expected utility of insurance. Romanosky, Ablon, Kuehn, and Jones (2019) looked at how cyber premiums are priced. We will combine and adjust the results and approach of these two papers to theoretically determine if an entity should insure; which retention rate is preferable and achieves the highest level of utility for an entity given a probability, industry, and revenue.

1.3 Cyber Insurance Market Today.

Today's cyber insurance market can be characterized as an emerging market where large companies initially have shown greater interest than small and medium-sized enterprises (SMEs) (N. Unhammer, personal communication, February 4, 2020; Franke, 2017). Arguably, large companies have adopted cyber insurance at a higher pace than SMEs, as large companies to a larger extent than SMEs have more professionalized risk assessment procedures and routines. Large companies also in, many cases, have a global organization, which is more dependent on digital solutions such as their internal cyber networks and IT-systems. The cyber risk of large companies is thus more severe when it comes to business interruptions, which can leave the better part of an organization paralyzed.

It is also arguable that it could be less complicated for an SME to continue operating their business manually or restore their digital solution in a state of emergency, compared to the more global and complex structure often observed in larger companies.

This, however, does not mean that SMEs are exposed to less risk than large companies. Large companies have their own IT departments, IT- procedures and training, while small companies usually have less developed routines and digital systems, and no IT departments. A cyber attack on an SME may, therefore, pose as

a more severe risk compared to that of a large company. The lack of IT safety routines and inhouse IT competence in SMEs may also make the long term effect of cyber issues more time-consuming to resolve. Therefore, it can be argued that it is more critical for an SME to have cyber insurance compared to large companies.

The losses inflicted by a cyber attack on a large company will naturally be more significant in value compared to an attack on an SME, but the SMEs losses are according to ESI Thoughtlab (2019) larger in percentage of revenue relative to the losses in large and very large companies (See Table 1).

2 Literature Review

2.1 Cyber Insurance Market

2.1.1 Incentives and Barriers of the Cyber Insurance Market in Europe

In June 2012, the European Network and Information Security Agency (ENISA) published a paper on the incentives and barriers of the cyber insurance market in Europe. They found that the drivers for the demand side of the cyber insurance market are rooted in companies' need for privacy, mitigation of post-attack costs, and reputational risk. ENISA also found indications that the cyber insurance market in Europe is small compared to the US market, justified by just a handful of carriers offering cyber insurance in Europe, compared to 30-40 in the US. Further on, ENISA point to the lack of data, the perception that existing insurance products are sufficient to cover the cyber risk, uncertainty in predicting future losses, and the lack of adequate reinsurance, as some of the main obstacles in the academic literature regarding cyber insurance. In addition, to point out obstacles in the cyber insurance market, ENISA also points out several incentives, such as lowering premiums through demands of higher IT security, given a causal link between the two, processes to set IT security standards for underwriting, certification of IT security products and services, etc. Furthermore, ENISA explains that the main incentives can be linked firstly to the expectations of better ways to determine the most effective risk-reducing measures. In turn, this could stimulate a range of secondary markets due to increased supply, as the cyber insurance customers would become "a better" risk for the insurance carriers.

Lastly, ENISA proposes four recommendations for future research and investigation.

- Firstly, they propose a collection of empirical evidence to increase the quantitative empirical work on prices, volume, or losses.
- Secondly, they suggest looking into if changes to European consumer rights legislation could affect companies' willingness to improve their risk management practices, rather than using cyber insurance to manage reputational damage.
- Thirdly, they recommend looking into if frameworks for the measurement of information value would lead risk managers to better value or price information assets, and in turn, be able to better consider insurance as a tool to support the company's activities.
- Lastly, they recommend looking into whether it would be possible to implement a public policy which would intervene by setting itself as an insurer of last resort (ENISA, Robinson & Rand Europe, 2012).

2.1.2 The cyber Insurance Market in Sweden

Ulrik Franke, a senior researcher at RISE (Research Institutes of Sweden), published a characterization of the Swedish cyber insurance market in 2017 by using semi-structured interviews with insurance intermediaries, insurance- and reinsurance companies. According to Franke, this essentially amounted to all companies selling cyber insurance in the Swedish market. He found that the coverages offered included discrepancies in the underwriting processes used. He also found that the typical annual premium for cyber insurance is in the range of 0.5-1% of the indemnity limit (Franke, 2017, p.130). Franke found that the insurance companies impose requirements for information- and IT security upon their customers and do not insure those who are immature or lack the required security. Thus, Franke argues that cyber insurance is not only a medium for risk transfer but also includes elements of avoidance and mitigation. He also found that his sources all agreed that among the Nordic countries Sweden and Denmark are the more mature markets, with Finland somewhere in the middle and Norway to some extent trailing behind (Franke, 2017, p. 136). In addition, the Swedish cyber customers are, for the most part, large companies.

2.2 Policies

2.2.1 Optimal Insurance Policies

Multiple articles are defining optimal insurance policies and coverage. George G. Szpiro, stated in 1985, that one of the more important findings is "that coverage decreases when risk premium increases." (Szpiro, 1985, p.1). George Szpiro's paper enhance this by using a mathematical approach to take a more explicit look at optimal choices of coverage based on different assumptions. The paper is concluding that different assumptions will influence the choice of coverage. Szpiro references Artur Raviv's research from 1979, which concludes "that the pareto optimal insurance contract involves a deductible and coinsurance of losses above the deductible."(Szpiro, 1985, p.1). Raviv's article also states that the coinsurance is a byproduct of risk or cost-sharing between the insurer and the insured (Raviv, 1979). These two articles represent only a small part of the literature which has been researched on the subject and the formulation of insurance policies and relevant aspects.

2.2.2 Premium Calculation and Insurance Pricing

An essential part of insurance theory is the calculation of insurance premiums. Roger J. A. Laeven and Marc J. Goovaerts published a paper in 2007 explaining classical theories and their generalizations. As well as summarizing the main issues and results, and outlining current advancements on the subject, Laeven and Goovaerts define the price of insurance, also known as a premium, as "the monetary value for which two parties agree to exchange risk and "certainty""(Laeven & Goovaerts, 2008, p.2). They also list properties that the principal of premiums may or may not satisfy.

2.2.3 Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk?

There exist much theoretical literature about cyber insurance. Still, there is little practical and qualitative research available about the content of the cyber insurance policies, and how the carriers price the cyber policies premiums. Sasha Romanosky, Lillian Ablon, Andreas Kuehn and Therese Jones (2019) therefore conducted a

systematic qualitative analysis of cyber insurance policies filed with the state insurance commissions to answer the following three questions;

i) What losses are covered by cyber insurance policies, and which are excluded?
ii) What questions do carriers pose to applicants in order to assess risk?
iii) How are cyber insurance premiums determined - what factors about the firm and its cybersecurity practices are used to compute the premiums?

This paper is the first systematic qualitative analysis of the underwriting process for cyber insurance. At the same time, the authors uncover how insurance companies understand and price cyber risk. The sample size is determined by thematic saturation; there was collected 235 filing dockets filed in New York, Pennsylvania, and California between 2007 to 2017. These dockets consisted of a zipped file that usual contained dozens of individual documents, which could include, among other things, coverage and exclusion forms, security questionnaires, and rate schedules. There is very little information available for the public on the content; thus, there is a lack of transparency in the underwriting process of cyber insurance policies (Romanosky, Ablon, Kuehn & Jones, 2019).

2.3 Cyber Insurance

2.3.1 What do we Know About Cyber Risk and Cyber Risk Insurance?

In 2016 Martin Eling and Werner Schnell summarized research on what was known about cyber risk and cyber risk insurance. They aimed to establish a database on studies, articles, and working papers on cyber- risk and insurance, with a focus on the business and economics literature in the field of risk and insurance. They use a standardized search and identification process to create a database of 209 papers, where the primary research results are extracted. Through this database, they conclude that there does not exist any established model for cyber risk. They further argue that this may be due to the lack of data on the matter, most likely because entities who have been affected often do not disclose incidences. This lack of data leads to challenges in risk management and the insurability of cyber risk (Eling & Schnell, 2016, p.474). They outline three significant insurability challenges of cyber risk; First, the independence and predictability of losses are not given, leading to risk pools not always working correctly. Secondly, challenge with information

asymmetry, in the sense that companies which already have been attacked, are more likely to buy cyber insurance, hence leading to adverse selection. Lastly, they point to the challenge of moral hazard through changed behavior after buying insurance, for example, in the form of less incentive to invest in self-protection measures. When it comes to future research, Eling and Schnell state that the existing research in 2016 was mainly focused on the supply side of insurance, while there were left much room for research on the demand side of cyber insurance. As for the future of cyber insurance, the authors argue that the market is still in its early stages, but there have been several new entries into the market. Therefore, one can expect risk pools to grow and more data to become available. In turn, this will increase insurance capacity and drive prices down. Lastly, they argue that it may be important to establish standards on definitions, coverage, and underwriting risk assessment, to reduce some of the current problems in the cyber insurance industry.

2.3.2 Insurability of Cyber Risk: An Empirical Analysis

Christian Biener, Martin Eling, and Jan Hendrik Wirfs researched the insurability of cyber risk using an empirical analysis approach, and systematically reviewing these results in the light of the insurance criteria set by Berliner in 1982. They are supporting the understanding that there are problems with the insurability of cyber risk and the creation of a sustainable cyber insurance market, due to "highly interrelated losses, lack of data and severe information asymmetries" (Biener et al., 2015, p. 131). They especially point to the lack of data and the need for more elaborate research on cyber insurance, to be able to develop necessary models and create sustainable cyber insurance policies. The empirical analysis in light of the Berliner insurability framework finds that the leading difficulties are the randomness of loss occurrence, information asymmetry, and the cover limits (Biener et al., 2014, p. 148). Taking into account the result of the analysis, they suggest the establishment of "minimum standards on coverage limits and pre-coverage risk assessment as well as clear-cut definitions of cyber risk" (Biener et al., 2015, p. 149). This can be viewed as a proposed solution to eliminate some of the problems related to the insurability of cyber risk.

2.3.3 Insurance when the Internet goes Down

Gerking and Smith addressed the problem caused by traditional length on waiting periods in cyber insurance policies in their article from 2017. They looked at the most significant DDoS attack to have ever hit a US company. The attack consisted of several separate attacks, which was fully resolved within 11 hours. Therefore, they argue that a traditional waiting period of 12-hours (or more) is not adapted to the cyber risk currently faced by companies.

They justify this through two arguments;

- Firstly, they argue that 12 hours is a substantial time not being able to conduct business over the Internet, implying that the waiting period is too long for the kind of risk being insured.
- Secondly, they argue that today's policies and their carriers would argue that since there were several separate attacks, they should also be viewed and treated as separate claims.

None of the individual attacks come near the 12 hour waiting period. Gerking and Smith also stated that since the attack affected a provider of services (third-party provider), few or non of its customers were affected for the full duration of the attack. They concluded that the waiting period and the limited business interruption coverage of cyber insurance policies are two significant limitations to cyber insurance policies.

2.3.4 Effect of Cyber Insurance on Social Welfare

A substantial amount of previous research on cyber insurance has focused on the definition of cybercrime and its effect on the market. Through this paper, Kuru & Bayraktar (2017) aims to analyze the relationship between cyber insurance and social welfare, and at the same time, compare it among three countries; USA, UK, and Turkey. The paper answers two cyber insurance questions: "What kind of contribution does cyber insurance make to social welfare?", and secondly "what kind of problems do insurers and insured have to face?". To do this, the authors use the model from Kesan, Majuca, and Yurcik' (2006) paper, to measure the welfare gains and losses of cyber insurance at different probabilities and risk levels. Due to the lack of available data, the model in this paper views countries as firms and measures changes in GDP for different risk and probability levels. By doing so, the

paper can illustrate the utility gained or lost by purchasing cyber insurance, which in turn is dependent on whether or not an attack happens.

The paper also looks at the optimal premium for cyber insurance, here the paper uses models developed by Cochrane (1997) and Kesan et al. (2006) to calculate the maximum amount insured would be willing to pay at different risk levels and attack probabilities. This was done by identifying the effect of welfare, which makes it possible to state the optimal trade-off between expected gain and level of risk. To understand the full effect of cyber insurance, the authors also measure the welfare loss that can occur due to adverse selection.

In insurance, there are two types of insured; high-risk and low-risk insured, which can differ by their probability of risk and attack. In an insurance market with adverse selection, the insurers are not able to distinguish between the low- and high-risk insured. In that case, the insurer will offer full insurance to the high-risk customers but cannot offer full insurance to the low-risk customers. This is because the high-risk customers under the adverse selection problem will have an incentive to mimic the low-risk customers and purchase the low-risk insurance. Thus, low-risk insurance will be more expensive than it should be, leaving the low-risk customers without insurance. This leads to a welfare loss for the low-risk customers, that would not be present without adverse selection. The authors calculate this loss as the difference between having an ideal cyber insurance policy and a condition somewhere between having no insurance and having a cyber insurance policy.

Lastly, the paper concludes that cyber insurance would have a positive impact on social welfare by making the Internet safer for all users. The result of the analysis shows that the problems of adverse selection can be eliminated with an accurate risk assessment, leading to appropriate premium levels for the insured (Kuru & Bayraktar, 2017).

2.4 Cyber Data and Market Challenges

2.4.1 The Cybersecurity Imperative Pulse Report

ESI Thoughtlab is an innovative thought leadership firm that generates insight through rigorous research and economic analysis (ESI Thoughtlab, 2020). ESI conducted an annual survey on the topic of cyber security in 2019. They gathered information from 467 companies in 17 countries with a distribution of roughly 20% mid-sized- and 80% large-sized companies within several different industries. In their 2019 survey, they found that companies see the Internet of Things (IoT) as the most significant vulnerability to their IT infrastructure. ESI also states that the rapid innovation within IT development, such as IoT and cloud technology increases corporate cyber risks if safeguards or precautions are not built into the systems upfront.

Older technologies such as email servers, laptops, out of date software, weak authentication, and user errors also pose a substantial risk for companies.

Further, ESI argues that companies are becoming better at identifying vulnerabilities and that they allocated around a quarter of their cybersecurity budget to risk identification in 2019. ESI also states that cyber vulnerabilities vary depending on the industry. They found that industries that have adopted the IoT have started to move away from sourcing technology based on price, and towards sourcing based on security. This shift in sourcing is a result of the realization of the risk of the IoT after several high-profile attacks through IoT devices.

When ESI compare their 2018 survey with the survey from 2019, they see that companies report higher losses from cyber attacks. However, these losses are in line with the increase of the number and size of cyberattacks across the different industries. They also state that the increase in losses reflect better corporate systems for detecting attacks and measure costs. As a result of this ESI sees an increase in companies estimates of cyber attack losses.

The survey found the following average difference in cyber losses between company sizes:

	Average revenue	Average loss	Loss as % of revenue
Mid-size	$600 million	$1,556,250	0.259%
Large	$4.4 billion	$3,309,375	0.076%
Very large	$26 billion	$10,773,423	0.042%
Average	$8.75 billion	$4,738,115	0.114%

Table 1 (ESI Thoughtlab, 2019, p.9).

2.4.2 Enhancing the Role of Insurance in Cyber Risk Management

The Organisation for Economic Co-operation and Development (OECD) (2017) provides an overview of the main challenges to the development of the cyber insurance market in terms of both insurers' willingness to provide coverage and the companies' demand for insurance coverage. To understand the challenges of the insurers OECD point to three criteria which is generally needed to ensure that the insurability of risk is economically viable;

- The risk must be quantifiable.
- A sufficiently large community to share risk must exist.
- Risk must occur randomly.

The extent to which the character of a given risk meets these criteria (among other factors) will impact whether insurance companies can collect the premiums necessary to cover the potential total losses of a community of insured. One can thus use these criteria to analyze the current cyber insurance market to find factors that may prevent the development of the market. Through an OECD questionnaire on cyber risk insurance, OECD found that of 36 insurance sector respondents, about two-thirds identified the ability to quantify cyber exposure as a concern. They argue that this is mainly due to the lack of historical data, the changing nature of cyber risk and lack of access to corporate security information, which is needed for underwriting individual risks.

Further, OECD states that the accumulation of risk is by some reports argued to be the primary reason that insurers limit the coverage for cyber insurance. Their own questionnaire found that respondents identified the accumulation of risk as one of the most important drivers of cyber risk. They point to the possibility of a catastrophic event, such as the exploitation of a weakness in a commonly used software or system. In such an event, losses would be correlated across insured and

lead to accumulation of risk, which the insurance market may not have the capacity to handle, thus leading to numerous exits from the market.

On the demand side of cyber insurance, OECD point to several factors that may reduce the demand and willingness to pay for cyber coverage such as companies not having awareness regarding the potential losses from cyber risk. Several recent studies carried out in Europe, show that the level of awareness of cyber risk and the senior management's attention to these risks have increased. However, the studies show that there seems to be a gap between the increased awareness of the risk and translating this risk into estimates of potential losses, which would normally be the starting point of the insurance acquiring process.

Another critical factor is that companies misunderstand or are not aware of the available level of coverage for cyber risk. This applies to both coverages from standalone cyber policies, but also from coverages provided by more traditional policies. This leads to companies not being able to determine what coverage gaps they currently have, and thus leading to low cyber insurance take-up in the market. Figure 1 is an illustration off the potential overlap of coverage between standalone cyber policies and traditional policies;

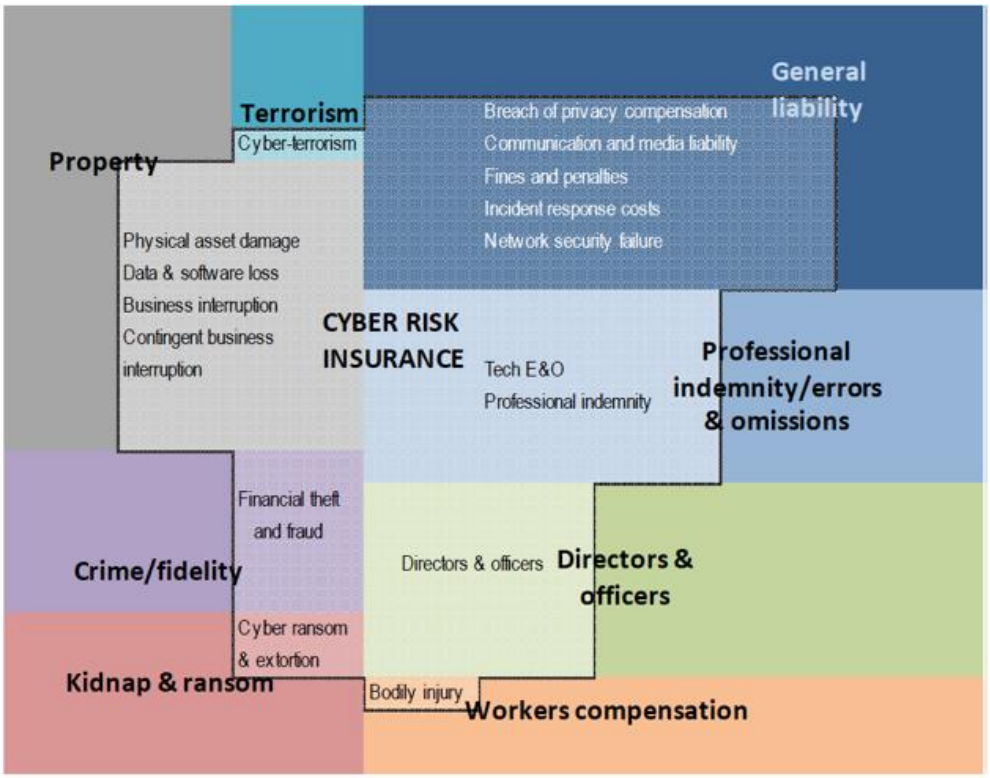


Figure 1. Source OECD on JLT Re (2017)

The last factor to which OECD gives attention, is the mismatch between the offered coverage and what the companies are seeking. A global survey of companies found that 36% of respondents stated that inadequate coverage relative to exposure was a significant driver to not acquire cyber insurance. Another UK survey found that 77% of companies meant that cyber insurance only partially met their needs for coverage. These studies did not identify why the companies' needs were not meet by the insurance, but reasons such as limited coverage for reputational damages and intellectual property theft can be likely reasons.

2.5 Summary of Literature Review

In general, the existence and hence the research of cyber insurance is relatively new. Still, a fair amount of research on the topic has been carried out, with the main focus being on theoretical research and models rather than on empirical research. The available literature, therefore, in many cases, lacks definitions and standards based on empirical research and practical examples. However, it often encourages future research to do so. The currently available research is provided by both organizations and researchers. As the cyber insurance market and amount of relevant examples of cyber attacks will grow over time, the availability of data and information will increase. In turn, the available data will be extensive enough to conduct more in-depth detailed analyzes. It can, therefore, in the future, be expected that the current theoretical research will be accompanied by an increasing number of papers based on empirical research.

3 Theoretical Framework

3.1 Definitions

Marotta, Martinelli, Nanni, Orland & Yautsiukhin (2017) provided structure for definitions related to insurance. The structure is meant to provide an understandable context and basis for insurance and cyber insurance. We specify definitions for what is defined as the actors, risk management, insurance policies, retention, cyber risk, and relevant aspects of cyber insurance.

3.1.1 The Actors

The principal actors in insurance are the insured and insurer. The insured is the actor who wishes to transfer risk and the insurer is the actor who assumes the risk for a given set of conditions. Insurance companies, also referenced to as insurance carriers assume risk in exchange for compensation. There are several other actors in the insurance industry, such as brokers, agents, and reinsurers. They provide different functions to support and enable insurance. In this thesis, we will refer to an insured party as an "insured entity" and an insurance company as an "insurance carrier".

3.1.2 Risk Management

Risk can be defined as exposure to adverse situations (Gupta, 2008, p. 3). The exposure to adverse situations indicates that the entity is exposed to a degree of uncertainty; the uncertainty is based on the assumption that a given scenario is either favorable or unfavorable. The occurrence of risk is defined as an incident. Risk is dependent on two aspects:

1. Threat, which states the cause of the risk such as an explosion or defective products.
2. Vulnerability, which is a weakness that can result in an incident, such as poor maintenance (Marotta et al., 2017, p. 39).

As a consequence of an incident, there could be a loss of wealth or other assets; this is defined as an impact. The impact can be both tangible such as damage on machinery and intangible such as loss of reputation and intellectual property (Marotta et al., 2017, p. 39).

We can hence conclude that risk exists if there are a cause, possibility, and consequence; in other words, there is a threat, vulnerability, and impact. As such, risk can be illustrated with: Risk = Probability x Impact (Marotta et al., 2017, p. 40)

"Risk management is an integrated process of delineating specific areas of risk, developing a comprehensive plan, integrating the plan, and conducting an ongoing evaluation."(Gupta, 2008, p.9). Risk management can, therefore, be broken down into three components, risk analysis to identify and evaluate the different risks. Risk control to avoid, eliminate, mitigate and limit severity as well as risk financing to

transfer or reduce risk. Thus, risk management can be concentrated to the notion that it is meant to either reduce probability or impact, which decreases the risk as illustrated in the above quantitative function.

Insurance is a contractual transfer of risk, a method of risk financing. When an insurance carrier agrees upon an insurance contract with an insured, the carrier agrees to indemnify their losses if an incident occurs. Thus, for a set of terms and conditions, an insurance carrier agrees to share some of the risk. In return, it charges a given price for assuming the risk transferred, referred to as premium (Gupta, 2008, p.12).

3.1.3 Insurance Contract

Insurance policies are a contractual agreement between an insurer and insured, facilitating for a transfer of risk. Insurance policies include Terms and Conditions which both an insured and insurer shall adhere to. The policies also include premiums, exclusions, coverage, and other provisions specific to some set of insurance agreements. Coverage is the amount of risk and liability that will be transferred to the insurer. Exclusions provide exclusions to the coverage.
For example, may an insurance contract for the destruction of property provide cover for a factory fire but exclude damage caused by a flood due to an exclusion in the policy of destruction by extreme weather (Marotta et al., 2017, p. 40).

Insurance coverage consists of two umbrella-terms for coverage, First- and third-party loss. The first-party loss consists of losses that are attributed to the insured' own losses, while third-party loss is the loss inflicted upon another entity. Property damage and business interruption are often what is classified as first-party loss. While third-party loss covers damage inflicted upon another entity such as liability claims (N. Unhammer, personal communication, February 4, 2020).

3.1.4 Retention

Retention moderate the insurers risks by placing a financial responsibility on the insured, which may limit risky behaviors, such as moral hazard. Moral hazard is defined as the risk of misusing services or goods on the assumption that the insured is detached from the risk after entering into an insurance agreement with an insurer (Wolferen, Inbar & Zeelenberg, 2013). Retention reduces the premium, hence the

cost of insurance for the insured entity, as the entity assumes responsibility for some of the cost of a claim (Burnecki, Nowicka-Zagrajek, Wyłomańska, 2005, p. 427). Risk-retention in insurance may refer to several different methods of retaining risk; it is most commonly defined as either a deductible or time retention, i.e., waiting period (Insurance Information Institute, n.d.).

3.1.5 Cyber Risk

While there is not yet a universally accepted definition, Cebula and Young (2014, p.1) defined cyber risk as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems". Consequently, stating that "cyber" consists of two elementary components, electronic communication *networks*, and *virtual reality*. These two elements are what differentiates cyber risk from other risk domains. Virtual reality relates to the intangible disposition of cyber risk and the following complex nature of assessing the implications. Networks are closely related to the cyberspace and refer to networks which agents connect to, including what is described as offline- and online networks (Eling & Schnell, 2016).

What separates cyber risk from traditional risk is the high-correlation and aggregation of risk due to the interconnectivity between actors, due to the global reach and nature of connectivity as a result of IT-systems (Ogut, Raghunathan, & Menon, 2011; Böhme & Kataria, 2006). The monoculture of a few widely adapted IT-systems also increase the aggregation of risk. If there is a weakness or breach of one system, this may be abused and affect several other users of the same system. Monoculture and the high interconnectivity negates the non-correlation of traditional risks such as geographical limitations, which emphasize the complexity of estimating the scope of impact.

Cyber risk is composed of different threats; Cisco summarizes these. Among these are malware attacks, which is malicious software, including spyware, ransomware, viruses, and worms. Malware breaches the network through a vulnerability. Phishing attacks can be explained as sending fraudulent communication and making it appear like a legitimate source of communication. The goal of a phishing attack is to steal sensitive data and/or install malware on the victim's machine. A

Denial-of-service attack (DoS) is when the attacker floods the systems, servers, or networks, thus exhausting the resources and bandwidth. (Cisco, n.d.)

3.2 Properties of Cyber Insurance

Compared to the development of more traditional insurance, the complex conditions of cyber risk complicate the development of cyber insurance. The impact and the likelihood of an incident are especially heavily influenced by the unique properties of cyber risk, thus skewing the estimates and development of cyber insurance.

3.2.1 Impact

There is a lack of limits due to the properties of cyber risk; this further complicates how insurers estimate the impact. Due to the monoculture of IT-systems and the aggregation of risk, the correlation between incidents may be higher than for insurance in general. The cyber incident may result in indirect consequences and a cascading effect on tangibles and intangibles (Frumento & Dambra, 2019, p. 58). Frumento and Dambra (2019) further elaborate on how cyber incidents may have comprehensive consequences for intangibles. This further complicates the effort to estimate the impact due to the nature of intangibles and the difficulty with quantification of intangibles such as reputation and intellectual property and related "damage" (Toregas & Zahn, 2014). Therefore, Toregas & Zahn (2014) conclude that it is difficult to estimate the accuracy of how extensive and significant an incident could be.

3.2.2 Probability

It is challenging to estimate the probability of a cyber incident occurring. This is due to the challenging aspect of estimating the impact, the accelerating technological development, lack of data, and information sharing (ENISA et al. 2012; Eling & Schnell, 2016; CISA, 2019). CISA (2019) state that the lack of information sharing inhibits the development of adequate tools and intensifies information asymmetries between the insurer and the insured. Further complicating the estimation of the probability is the sheer number of incidents occurring, Hiscox discovered in their 2019 survey, that 61% of their respondents have experienced a cyber incident (Hiscox, 2019).

3.2.3 Coverage

Cyber insurance first-party coverage will cover losses incurred directly by the insured. Such costs could be destruction of property, loss of information, financial loss due to cyber extortion, business interruption, and PR-costs. While Third-party coverage, cover costs arising from third party losses. This could be losses due to data compromises, loss of third-party data and private information, defense -and settlement costs, costs related to litigation, fees, and fines (Romanosky, Ablon, Kuehn & Jones, 2019).

The interdependencies of the global and modern digital cyber world highlight the risk of overwriting cyber insurance. Cyber risk concerns related to insurance involves high accumulation of risk due to the high correlation. As was illustrated in the case of the NotPetya attacks, several companies in different industrial sectors spanning different continents were hit simultaneously (Greenberg, 2018). This emphasizes the flaws of writing cyber insurance against cyber risk in different sectors to mitigate the accumulation of risk and offset total losses.

3.2.4 Information Asymmetry

Information asymmetry could be referred to as a situation where an entity does not have access to the same information as another entity. Marotta et al. (2017) describes in their paper that insurance works sub-optimal when there is high information asymmetry between the insurer and insured. This is emphasized as there is a strong presence of information asymmetry due to adverse selection and the Moral Hazard dilemma. Adverse selection, where companies that have experienced a severe cyber incident are more likely to purchase cyber insurance (Shackelford, 2012), and Moral Hazard, meaning that companies may be inclined to invest less in cybersecurity due to the presence of cyber insurance.

3.3 Insurance Market

To understand the evolution of the cyber insurance market, one have to understand how the insurance market develops, writes, and, in some instances, tailor insurances to customers. This process involves several participants, whereon the principal actors of the insurance market can be divided into six separate segments.

- The demand side, companies pursuing insurance
- Insurance carriers
- Insurance- and reinsurance brokers
- Insurance agents
- Reinsurance companies and syndicates
- Regulatory authorities

Insurance Brokers

Insurance brokers work for the insured entity or would-be insured. This was clearly stated by law and formulated by Lord Justice Hobhouse (Zhang, 2014). As an agent of the insured or would-be insured, this involves advising the entity on different domains. Such domains could be coverage, advising on exposure to risks, and working with insurers during a tender-process (CIAB, n.d). During the acquiring process of insurance, a would-be insured will enter into a contract with an insurance broker. The insurance broker will examine the needs of the would-be insured, present possible insurers and relevant products and assist in the tender process. Furthermore, insurance brokers may be of assistance during an incident which may require further scrutiny, or if the insurance terms have been triggered and there is a need for negotiations.

Insurance Agents

Opposed to insurance brokers, insurance agents are licensed to conduct business on behalf of insurance carriers. The agents hence represent the insurance carrier in the insurance process and generally operate under the terms of what is called an agency agreement. The insurer-agent relationship can take several forms; independent, exclusive, insurer-employed, or self-employed. An independent agent works on contract with several insurance carriers, whereas an exclusive agent either works with one insurance carrier or sells a single type of policy from several carriers. A self-employed agent is independent of carriers and can sell any insurance product from any carrier. On the other hand, an insurer-employed agent can "only" sell insurance products from the carriers he/she operates with (CIAB, n.d)

Regulatory Authorities

To understand why the insurance market is regulated, it is necessary to understand the purpose of regulations. In a broader aspect, regulation can be defined as the imposition of rules by the government, which is backed by the use of penalties that are meant to modify the economic behavior of individuals and firms in the private sector (OECD, 2018). OECD (2018) further explains an insurance regulator as any authority that initiates and develops legislation and/or non-legislative regulation (i.e. rulemaking). These legislations and regulations are meant to ensure that the interests of policyholders are protected. The insurance market's stability and robustness are promoted and inappropriate behavior by insurers, reinsurers, and affiliated service providers is avoided (p.13).

Reinsurance Companies and Syndicates

To provide an economically sustainable policy, an insurance carrier must be able to offer the policy to a wide range of insured entities, to achieve a positive net revenue through the accumulation of premiums. However, when accumulating a large pool of policies, the total risk pool will grow proportionally (Emrich & Czajkowski, 2013). If there is an incident requiring the insurance carrier to indemnified multiple policyholders simultaneous, and the accumulated premiums do not cover the total amount, a reinsurer will then provide financial support to the insurance carrier. This, in practice, is when a reinsurer operates like an insurer for the primary insurance carrier. Reinsurance companies provide an effective risk transfer mechanism for insurance carriers, and allows the carriers to write insurance for large, accumulated, and complex risk (Pohl & Iranya, 2018, p.7). Reinsurance syndicates, a group or pool of insurance carriers and/or reinsurers, provides an enhanced ability to offer coverage for highly risky liability exposures such as cyber risk.

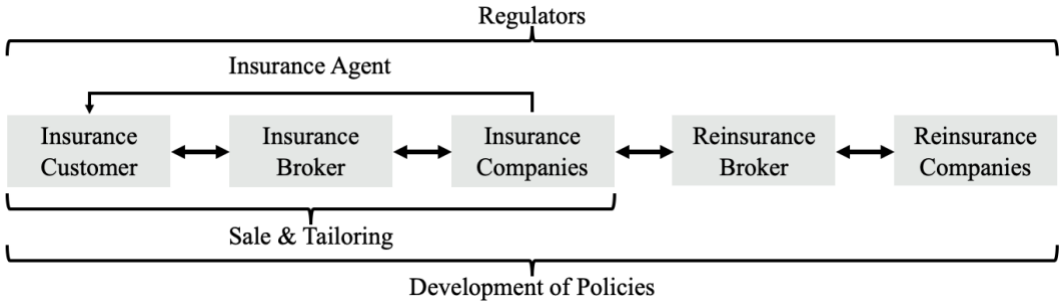


Figure 2 - The Insurance Market

3.3.1 Insurance Industry

Where the "insurance market" can be used as a terminology which include all the actors within insurance, the "insurance industry" is used for the specialized professional part of the market, i.e., the brokers, agents, insurance carriers and reinsurance companies.

The insurance industry' product-channel can be divided into two key components, namely the development of policies and the sale and further tailoring of the policies terms and conditions, as illustrated in figure 2. If organizations or companies wish to obtain their own program instead of an operator program, the two main components merge into one integrated process.

The process of developing new insurance products involves the entire insurance industry. The development of a new insurance product starts when there is an inadequacy in the current products to meet the emerging demand. Insurance carriers then estimate whether there is an economic incentive to provide products to the emerging demand. To do this, the insurance carriers cooperate with the insurance brokers to understand their customers' demands. Further on, the insurance carriers collaborate with reinsurance companies to receive access to their experience, leverage their data to estimate the unknown risk, the pricing of premiums, and the establishment of reinsurance pools. For traditional insurance products, insurance- and reinsurance companies have several years of cumulative experience, data, and understanding of cause and effect. Thus, insurance companies have arguably adequate tools and abilities to accurately estimate the risk related to traditional insurance elements and price premiums "correctly". For instance, the industry has an approximation to the probability of a fire in a specific building due to earlier incidents, geographical knowledge, known parameters, and the likelihood of the fire spreading to nearby buildings. Hence, insurance companies are confident in their risk estimates and can adequately calculate a premium proportional to their beliefs of the risk (N. Unhammer, personal communication, February 4, 2020) In the case of cyber insurance, the existing tools and data are not sufficient for the insurance companies to estimate risk and price-related premiums confidently.

There are two ways of calculating premium; actuarial data, and normative standards. For actuarial data the insurance carriers will take a retrospective look at historical data and statistics, while for normative standards, the insurance carriers

base their calculations on a causal relationship (Toregas & Zahn, 2014, p. 5). While actuarial data is not present for cyber risk (ENISA, Robinson & Rand Europe, 2012), there are some indications of normative standards, but they are not solid enough to be considered viable (Toregas & Zahn, 2014, p. 5). Therefore, Toregas and Zahn conclude that traditional insurance computation and the current estimation tools are not a good fit for the fast-changing, dynamic environment of cyber risk and the underlying information asymmetries of the industry.

The lack of proper fit and adequate modeling methods skews the estimation of risk for the cyber insurance market (Eling & Schnell, 2016). As a result of this, the insurance carriers are more dependent on reinsurers with knowledge in specialty products such as cyber insurance. The unknown parameters and dependency on some few large reinsurers influence the development of cyber insurance products in such a way that the products are more homogenous than what is conventional for traditional insurance products (N. Unhammer, personal communication, February 4, 2020).

Traditionally insurers carriers achieve profits by accurate pricing of insurance policies, where the profit-maximizing scenario is when the aggregated indemnity for a given interval is less than the accumulated premium. For cyber insurance, this relation is not yet been well examined and explained, mainly since little or no prior experience exists. Further complicating the case is the potential extent of cyber risk. It's substantially more extensive than that of traditional insured risks, as it's not dependent on elements such as traditional limitations and scope. A cyber incident could affect several parts of a global business simultaneous, compared to the "one incident, one segment affected" of traditional risks. Due to the lack of experience and data, both the insurers and the reinsurers are reluctant to take as much risk in a cyber policy, compared to traditional policies. Hence risky policies need several insurers and reinsurers, resulting in need for insurance syndicates (N. Unhammer, personal communication, February 4, 2020). The uncertainty regarding the potential risk facilitates for high premiums, low coverages, and ambiguous inclusions, due to the insurers and reinsurers need to mitigate and rationalize risk (Biener et al., 2015; Eling & Schnell, 2016). The uncertainty, homogenous products, and high premiums create suboptimal product offerings for the insured or would-be insured and a suboptimal market for the insurance- and reinsurance companies.

3.4 Business Interruption

Business interruption is defined as a period when a business cannot operate due to an unforeseen event (Cambridge Dictionary, n.d.). During a business interruption, an entity can not provide, produce, or offer its goods or service until the interruption is finished. This can be illustrated by a manufacturer suffering a breakdown in the manufacturing machinery. The manufacturer will not be able to produce the planned output, thus enduring a loss of income.

An insurer will, therefore, offer business interruption insurance; this allows the insured to mitigate the consequence a business interruption has on income. Business interruption insurance encompasses coverage for losses directly caused by a loss-occurring event such as a fire, destruction of property, or DoS-attack (Schumann, 2013**)**. The insurer will compensate for the loss of business income sustained under the coverage period, which may be described as the "period of restoration". Often will insurers state a minimum time limit from when the business interruption coverage will start; this is defined as the waiting period.

3.4.1 Waiting Period

A waiting period is a method of risk retention that can be explained as a contractual agreement on the time between the trigger of an insurance event (claim) and the period of restoration. Given that there is contractual agreement upon the waiting period, the insurance carrier will not compensate for any losses during the retention period. As is one of the objectives of retention, is to act as a buffer for the insurance carrier, so the carrier is not involved in minor incidents and claims (Burnecki, Nowicka-Zagrajek, Wyłomańska, 2005, p. 427).

For business interruption coverage for insurance in general, the waiting period is typical between 24-72 hours (Marsh, 2012). While for cyber insurance, the waiting period for business interruption coverage will vary between 8-24 hours, as stated by the policies which have been gathered for this thesis and interviews with industrial professionals. As for most elements in insurance policies, there is possible to negotiate a lower or higher waiting period; this will, however, affect the premium. Hence, the considerations related to the length of the waiting period is, in essence, a premium question.

3.5 Utility Theory

Utility is defined as the satisfaction which a consumer can obtain from a good or service. Total utility is a theoretical and conceptual term to measure several units of utility a consumer may gain from consuming a given good or service (University of Minnesota Libraries Publishing, 2011). The expected utility can, therefore, be defined as the utility which a consumer is expected to obtain, given a specific alternative occurring. The utility can, thus, be used as an indication of the amount of wealth and utility that different choices may provide. This may simplify a decision-making process, by "reducing a complex situation into a comparison between "real" values" (Goovaerts et al. 2008).

The Von Neumann-Morgenstern utility function is one of the primary methods of analyzing the decision-making process in modern economic theory. We will look at a generic utility function U(W), this is a utility function which provides the utility for an agent (consumer) given a level of wealth. The Von Neumann-Morgenstern utility function takes into consideration two different outcomes. These outcomes may be classified as a good or bad outcome (Neumann & Morgenstern, 1944).
Attributes of the function are also dependent on the attitudes of the agent. The agent can either be risk-averse, risk-neutral, or risk-seeking.
A risk-averse agent will prefer alternatives with less risk. The risk-neutral agent will be indifferent to the alternatives and not have preferences. In contrast, a risk-seeking agent will choose the alternatives which contribute to the highest return, indifferent to the risks involved.

For insurance to be applicable, the agent must be risk-averse and therefore prefer the choice which provides less risk. Mathematically derived, this requires that the first derivate has to be increasing, which means that inequality is $U'(W) > 0$. This implies that the agent prefers a higher level of wealth. The second derivative is required to be $U''(W) < 0$; this indicates that the utility function is concave for a risk-averse agent. Concave utility function suggests that the marginal utility is decreasing for each new level of wealth.

Expected utility without insurance

Assuming that an agent is exposed to a loss L^e where the impact will have a P probability. For a probability of $1 - P$**,** the loss L^e will be zero (0), indicating that there is no impact. Thus, an agent without insurance will for wealth ex ante an incident $W_1 = W_0 - L^e$. Following is the expected utility when there is no insurance:

$$E[U(W_1)] = p \times U(W_0 - L^e) + (1 - p) * U(W_0) \qquad (1)$$

Considering Jensen's Equality which states that for a random variable, in this case, L^e and a concave utility function, that

$$E[U(W_1)] \leq U(E[W_1]) = U(W_0) - E[L^e] \qquad (2)$$

Entities with a similar utility function will prefer to pay a fixed amount $E[L^e]$, instead of the random variable and volatile L^e, indicating that they are risk-averse (Goovaerts et al., 2008).

Expected utility with insurance

Assuming that an agent is exposed to a loss L^e, where the loss will have a P probability. For a probability of $1 - P$**,** the loss L^e will be zero (0), indicating that there is no impact. If an agent buys insurance, the agent is being charged a premium, Premium γ for coverage S. An insurance contract can, therefore, be rephrased as (γ, S). Culminating in the following wealth ex ante for P, $W_1 = W_0 - L^e - \gamma + S$, and wealth ex ante for $1 - P$**,** $W_1 = W_0 - \gamma$.

If we assume that the insured obtains full cover in case of a loss event $S = f(L^e) = L$, while paying the premium γ. Hence the insurer will have an expected utility of:

$$E[U(W_1)] = U(W_0) - \gamma \qquad (3)$$

While the pure premium γ is assumed to be actuarially fair when the price of an insurance contract (γ) equals the expected loss (L) illustrated by the following relation (Autor, MIT & NBER, 2016):

$$\gamma = E(S) = E(L) \quad (4)$$

Considering equations (2) and (4):

$$E[U(W_0) - L^e] \leq U(W_0 - P) \quad (5)$$

Equation (5) illustrates that a risk-averse agent will prefer to purchase insurance to transfer the risk to an insurer for a fixed premium γ, instead of paying a random loss.

For the insurance contract to be acceptable for the agent, the $\gamma = E[S] * (1 + \lambda)$. Where λ represents a term for general expenses related to the insurer,and the premium process has to be low enough to ensure that equation (5) holds (Marotta et al., 2017).

4 Methodology

4.1 Methodological Approach

Going into the process of writing this thesis, the only certainty was the topic of cyber insurance. Due to the lack of preexisting knowledge on the topic, we struggled to narrow it down into a suitable research question. Initially, the aim was to look at how cyber insurance could have impacted the cyber attack of Maersk in 2017, but it became clear that there was not enough publicly available information and data. Therefore, a process of collecting more information and data was needed. By analyzing existing research, academic papers, and insurance policies, as well as conducting interviews, a mixed-methods approach was utilized. This allowed for both quantitative and qualitative methods, which in turn supported numerical and in-depth exploration. The interviews were conducted in a deductive way, where industry professionals were interviewed.

This information gathering process helped in understanding what information was available and what the industry professionals saw as interesting and worth looking further into. This led to a research process more directed at how waiting periods and self-insured retention impact cyber insurance' effect on a cyber event. This was further narrowed down into the following research question; "how does cyber-

related business interruption fit to the modern cyber risk, and whether there exist a time retention level which provides a higher return for an entity."

The method used for the qualitative part of the research can be categorized as a thematic analysis with an inductive approach.

In addition to using qualitative data to answer the research question, a quantitative model was developed. This was done by analyzing the content of several carriers' cyber policies, then using the collected information to develop a model containing policies and information representative to the current cyber insurance market.

4.2 Methods for Data Collection

Since the thesis is based on a mixed-methods approach, it was natural to collect and analyze the data in stages, a so-called staged data approach. This is when one type of data is collected and analyzed before the next type of data is collected and analyzed (Harding & Whitehead, 2013, p.143). There are two stages; firstly, the conduction and analysis of three interviews. Secondly, the last stage consisted of the collection and analysis of cyber insurance policies. This step was influenced by the analysis and findings from the interview stage.

4.2.1 Interviews

To gain better insight into the cyber insurance industry and help develop a more specific research question, three independent, in-depth semi-structured interviews were conducted. One with an insurance professional, one with an insurance broker, and one with the head of insurance at Norsk Hydro ASA. All of the three interviews were recorded with consent and transcribed afterwards. The three interviews were set up by the supervisor of this thesis, Morten Lund.

The three interviews were conducted to help clarify how cyber insurance is viewed by its three most important actors; the insurance professional, the insurance broker, and the insurance customer/buyer.
The first interview was with Eirik Lund, an insurance professional at Gjensidige, a Norwegian insurance carrier. It was conducted at BI Norwegian business school campus in Oslo; it lasted for approximately 35 minutes.

The second interview was conducted with Nanna Unhammer, a senior broker at Willis Tower Watson Norway. Erik Rønningen was also present for some part of the interview. The interview was conducted at the Wills RE Nordics office in Oslo and lasted for approximately 75 minutes.

The final interview was held at Hydro's headquarters at Vækerø. It was conducted with Glennie Ingebrigtsen, Hydro's head of insurance. It lasted for approximately 70 minutes.

The transcriptions are enclosed in the appendices A1, A2, and A3.

4.2.2 Model

To determine the adequate number of policies to analyze, purposive sampling was used; this is a qualitative non-probability sampling method. This method is used due to the homogeneous sampling found in the cyber insurance policies, where most of the policies are quite similar. When using purposive sampling, the sample size is determined by thematic saturation. This means that data should be collected until no more patterns or themes emerge from the data (Research Methodology, n.d.). Romanosky et al. (2019) estimate the full population of cyber polices to be around 2000-3000, way above the analysis capabilities of this research effort.
The polices being analyzed are made for the US market. We can thus use Romansky et al.'s. (2019) analysis of the state-level insurance regulation in the U.S that suggests that there should not be any systematic variation across the states in regard to the content of the insurance policies. This does not mean that there are no differences between the policies, just that the differences that exist would not materially bias the results or conclusions. Following the analysis and findings of Romansky et al. (2019), we can justly view all US states as similar, supporting our data collection and a pooled analysis.

To collect data, we used the SERFF system in the US; this is an online database managed by the National Association of Insurance Commissioners (NAIC). This is a database intended to facilitate the submission, review, and approval of product filings between regulators and insurance carriers (SERFF, n.d.).

We collected only approved cyber policies and ignored those yet not approved or rejected. Since we only collected policies from SERFF, all policies are part of the

admitted market. In other words, the polices follow all state regulations and the carriers must file both their policies and rate schedules with the state insurance commission (NAIC, n.d.).

The policies analyzed span the years 2018-2020 and come from the following carriers; Berkley, Chubb, Everest National Insurance Company, National State Insurance, Philadelphia Insurance, The Hartford, The Travelers Companies (Travelers), and QBE Insurance.

4.3 Methods of Analysis

4.3.1 Interviews

The interview's primary purpose for this thesis was not to standardize, but to create more depth and nuance to the thesis. However, it is still a process where data is generated, and thus there is a need for some form of analysis. Thematic analysis was mainly used due to its independence from any particularly theoretical approach (Braun & Clarke, 2006), but also due to that, it allows for analysis in light of the research question. This was needed, as the interviews were conducted before the final research question was developed.

Braun and Clarke (2013) explain that a thematic method involves seven steps; transcription, reading and familiarization, coding, searching for themes, reviewing themes, defining and naming themes, and finalizing the analysis. They further state that by using this method, researchers can capture complicated, messy, contradictory relationships that prevail in the real world.

The transcribing of the interviews allowed us, as researchers, to become familiarized with the data. A careful reading then followed to ensure that the data was understood properly and that things of interest were noticed. By doing so, Braun and Clarke (2013) argue that it is possible to interpret data through the actual theoretical perspective of the thesis. As a result of this process, the following patterns and relationships were found in the interview data. All three interviewees state that cyber insurance is a relatively new product on the market and hence, lack customer awareness concerning its coverage and potential for risk mitigation, resulting in that some cases being seen as unnecessary by the customers. They also

state that the lack of data is one of the most significant barriers to the development of both the cyber insurance product(s) and the cyber insurance market.

Braun and Clarke (2013) describe a code as "a word or brief phrase that captures the essence of why you think a particular bit of data may be useful" (p.207). These codes can be data-derived or researcher-derived. The data-derived codes, which are called semantic codes, provide a concise summary of the explicit content. While the researcher-derived codes go further, by applying conceptual and theoretical frameworks to extract and identify implicit meanings from the data, these codes are called latent codes (Braun & Clarke, 2013, p.207). When analyzing the interviews using this approach, the main focus was to develop the latent codes; however, both latent- and semantic codes were found. The codes and analysis of the interviews can be found in the appendices A1, A2 and A3.

In the next step of the analysis, the codes are used to analyze and understand the patterns of the data. This is done by allocating the codes into sub-themes and themes. Braun and Clarke (2006) explain that a theme should capture something important about the data in relation to the research question and that it represents some level of patterned meaning or response within the dataset (p.82).
Both the sub-themes and themes are more extensive than the codes, in the sense that they contain many facets. An analysis of the codes from the data identified ten sub-themes, these sub-themes were, in turn, viewed and analyzed in relation to each other, resulting in four themes being identified.
When viewing the themes, it is important to understand that they are not supposed to cover every aspects of the data, but rather illustrate the data relative to the research question. Further on, the themes are not universal, in the sense that different perspectives and theoretical influences, may lead to the themes being analyzed and viewed differently.

Codes	Sub-Themes	Themes
• Influence of regulations • Role of regulators	Influence of rules and regulation	Regulatory requirements, support and demands imposed by cyber insurance policies
• Professional support • Demands put on customers.	Support and demands imposed by the insurance company	
• Lack of data • Lack of information • Lack of experience	Lack of knowledge	Lack of knowledge inhibits the development of the market and products.
• Emerging market • New treats • Coverages are trending upwards	Evolving market and products	
• SMEs lagging behind • Mainly for large companies	The current products are aimed at large companies.	The customers and internal and external factors influencing the development of the market
• Customers sensitivity to price • Lack of understanding of coverage • Process of standardization • Outsourcing functions	Customers do not understand their need for cyber coverage.	
• Influence of changing market conditions • Influence of subcontractors • Influence of experience	Influence of internal and external factors	
• Pricing and risk assessment • Risk potential • Damage estimation • Potential for damage	The drivers of cyber insurance	The drivers, structures, and roles of cyber insurance
• Coverage of CF • Structure of policy • Role of CF	Internal structure and demands of the cyber insurance	
• Role of reinsurance • Role of captive	Indirect actors in cyber insurance	

The last step of the thematic analysis involves presenting the themes and sub-themes in light of the research question "how does cyber-related business interruption fit to the modern cyber risk and whether there exist a time retention level which provides a higher return for an entity." as well as previous literature and knowledge on cyber insurance. By doing so, Braun and Clarke (2013) argue that the themes and sub-themes can contribute to and in some cases, answer the research question. Since a staged approach has been used, the interviews themselves are not meant to answer the research question alone. They are instead supposed to contribute to and support the results from the model. Due to the nature of cyber insurance, the discovered themes are intertwined, and they should thus be viewed in relation to each other. However, this does not prohibit them from being viewed independently.

4.3.2 Analysis of the Themes

Regulatory Requirements, Support and Demands Imposed by Cyber Insurance Policies

It is evident through this theme that the cyber insurance industry must comply by specific requirements and regulations. While the industry simultaneously impose demands on its customers. In 2012 ENISA stated that IT-security demands imposed by cyber insurance policies can be used as a tool to help manage the risk which is insured. For instance, stricter demands may lead to lower risk and hence lower premiums, while less stringent demands may lead to higher risk and higher premiums. The purpose is to make cyber risk a "better" risk to insure by ensuring that customers keep their IT-security up to date. This, in addition to factors indicating a lack of data and experience as well as new threats emerging, makes it evident that cyber risk is a dynamic risk, constantly requiring reviews and analysis to understand the present risk potential and how to best take mitigative actions against it. This results in the need to regularly consider the terms and conditions of the cyber insurance policy, supporting the need for a model to analyze the optimal choice of waiting period.

Lack of Knowledge Inhibits the Development of the Market and Products.

Factors such as lack of data, experience, and information, as well as cyber insurance being an emerging market with new threats, points to the possibility for adverse selection. Where it can be argued that companies who have already been subject to an attack will be more likely to acquire cyber insurance, compared to companies who have not experienced an attack. This is also supported by the findings of Eling & Schenell (2016), as well as factors such as customers lacking understanding of both the coverage and purpose of cyber insurance. This knowledge gap is also identified by the OECD (2017). These factors lead to that the customers can overlook the effect and importance of waiting periods. In addition, the lack of knowledge and understanding of how cyber risk behaves and how cyber insurance limits these risks may lead customers to make uneducated choices of waiting period. Thus, these factors and themes support the need to analyze the optimal choice regarding waiting periods for cyber insurance.

The Customers and Internal and External Factors Influencing the Development of the Market

The current market and available policies are focused primarily on larger companies; this is an important factor, due to the difference in how large- and SME companies are prepared to handle a cyber incident. The large companies often have in-house departments of IT-specialists and consultants on retainer, ready to support when an incident occurs (G. Ingebrigtsen, personal communication, February 13, 2020; N. Unhammer, personal communication, February 4, 2020). While SMEs are more dependent on the support provided through a cyber insurance (N. Unhammer, personal communication, February 4, 2020). There can thus seem that the importance of waiting period will differ depending on the size of the company. For a large company with plenty of resources to investigate, repair, and rebuild, the question of waiting period may not be as vital as it is for SMEs. SMEs, with fewer resources, may therefore, be more dependent on having external support included in its insurance policies. Due to the potential for cyber incidents lasting well beyond the attack itself. The question of where the cost of an attack occurs is important. This is supported by the factors of damage potential and estimation. Is the estimated/predicted cost of an attack, in the attack itself (implying a need for short(er) waiting period), or is it in the aftermath of the attack (implying a need for

long(er) waiting period)? This uncertainty supports an analysis of the optimal choice of waiting period.

In addition, OECD (2017) states that there currently is a mismatch between the coverage offered and what the customers want. This seen in relation to the factors of customers lacking understanding of the coverage offered, and at the same time, being sensitive to price can indicate that the utility of cyber insurance currently is not understood. This supports an analysis of the optimal choice of waiting periods, which can lead to a higher utility.

The Drivers, Structures, and Roles of Cyber Insurance

The thematic analysis uncovered several factors that create and drive the need for cyber insurance. It also uncovered uncertainty in several areas, such as the potential for risk and damage, as well as the role and coverage of cyber insurance. It can be argued that the industry's role and drivers are not understood or acknowledged by the demand side (the customers), resulting in a gap between the awareness of the potential risk and the estimation and mitigation of risk. This is supported by OECD (2017), which argues that this gap prevents the process of acquiring insurance, as companies underestimate their inherent risk. The understanding or lack of awareness of available coverages is also an important factor as to why cyber insurance is not adopted by companies, leading to suboptimal market conditions. A model illustrating the optimal choice for waiting periods can thus contribute to increased awareness of potential coverage and the adaptation of cyber insurance.

Through the codes, sub-themes, and themes, it is evident that the cyber insurance market is still underdeveloped. This is supported by factors such as emerging market, lack of data and experience, the process of standardization, and lack of understanding of the need for cyber insurance and coverage of cyber insurance.

It is also evident that the customers and the products offered are still adapting and evolving as new information and data are generated, gathered, and analyzed. In addition, the customers have not fully adapted to this form of insurance, either due to the lack of understanding of its function and coverage, it's price, or due to the policies targeting larger companies rather than SMEs. This supports the model's effort to investigate the utility of waiting periods, and by doing so, illustrating the effect cyber insurance can have on the implications of a cyber incident.

This in turn, supports the models' effort to further investigate the potential utility of cyber insurance waiting periods and thus, its potential to be embraced by the customers, which will allow the cyber insurance market to grow both its experience and its customer base.

4.3.3 The Development of the Model

The model was developed using underwriting guidelines and rates extracted from SERFF.
Underwriting guidelines are "a set of rules and requirements an insurer provides for its agents and underwriters. The underwriter uses these guidelines to make decisions regarding the acceptance, modification, or rejection of a prospective insured." (IRMI, n.d.b). The rates used are a complementary document to the underwriting guidelines, explicitly stating the rates used for premium calculation which apply to the specific conditions of an entity.

Microsoft Excel was used to create, run, and analyze the data for the model. Since this is a quite simple model, intended to illustrate the expected utility of having cyber insurance, there has not been applied any statistical methods, such as linear regressions or t-tests.

4.4 Justification of Methodical Choices

The interview with Eirik Lund was the most general out of the three interviews. As Lund is not an expert in cyber insurance, he contributed with general knowledge on the inner workings of the insurance industry and how the cyber insurance industry has developed globally and in Norway. However, this and the other two interviews contributed to future research and the development of the research question. The methodical choice of conducting interviews can thus be justified, as it contributed to the thesis's development and results.
Using thematic analysis to analyze the interviews produced a similar result to that found in existing research and literature. Therefore, this analysis method can be justified based on the integrity of the existing research and literature.

The gathering of policies, questionnaires, and underwriter guidelines was done to ensure that the data used was as up to date as possible. Existing research of similar nature was also used as support to the research. This was done due to cyber

insurance being an area characterized by high development and fast changes. A particular research method was not applied to the data, as the purpose was not to interpret the data but to extract it.

5 Model

5.1 Summary of the Model and the Models' Output

The model measures the expected utility of business interruption coverage in cyber insurance, given specific characteristics related to the insured entity and waiting period. The model intends to calculate the expected utility of revenue for an entity, with and without insurance. The expected utility of no insurance functions as a reference point, to measure the effect of insurance on expected utility, resulting in a difference between the expected utility of revenue when insured versus when not insured.
If the expected utility is positive, being insured will achieve higher return then not being insured, whereas when the expected utility is negative an entity should not insure. Which in turn will indicate if the given waiting period will have a positive or negative return for the entity.

We choose to look at the expected utility paradigm as a normative model for decision-making under uncertainty (Małecka, 2019, p. 36). Hence, the model explains how an entity should act when confronted with uncertainty regarding whether to insure or not. This is in accordance with an expected utility-related slogan, "choose the act with the highest expected utility" (Briggs, 2014). As defined earlier, utility enables an entity to make a comparison between two scenarios in a complicated situation using "real" numbers, establishing a ranking of choices (Kaas, Govaerts, Dhaene & Denuit, 2008, p.2). The intuitive process is that an entity will prefer the highest-ranked choice, i.e., the choice with the highest value of expected utility.

5.2 Expected Utility Explained by Case

We use the following example to illustrate a simple calculation of utility:

If an entity has a utility function U(w) where w is wealth, and has $1 000 000 in wealth, with a 10% possibility of a fire causing a loss of $200 000, the following expected utility(U), of the entity is:

$$E[U(w)] = Probability \times U(Wealth) + (1 - Probability) * U\big(Wealth - Fire(loss)\big)$$

$$E[U(w)] = 90\% \times (1\,000\,000) + 10\% * U(1\,000\,000 - 200\,000)$$

$$E[U(w)] = 980\,000$$

The expected utility of wealth given the probability of a fire is 980 000.

If the entity is given the choice to insure against fire, presuming that the insurance agreement covers an indefinite loss amount, for a $10 000 premium, implying that for this scenario loss = premium, the following expected utility (U), of the entity if insured(i**)** is:

$$E[U(w\boldsymbol{i})] = Probability \times U(Wealth - Premium) + (1 - Probability) * U(Wealth - Premium)$$

$$E[U(w\boldsymbol{i})] = 90\% \times (1\,000\,000 - 10\,000) + 10\% * U(1\,000\,000 - 10\,000)$$

$$E[U(w\boldsymbol{i})] = 990\,000$$

The expected utility of wealth when insured is 990 000.

$E[U(w)]$: 980 000 $< E[U(w\boldsymbol{i})]$: 990 000

Based on the theory of expected utility as a tool of ranking the most “choiceworthy” act (Briggs, 2014), the entity will prefer to be insured, thus choosing to insure when $E[U(w)] < E[U(w\boldsymbol{i})]$.

5.3 Expected Utility Function of Business Interruption Insurance

5.3.1 Good State and Bad State

For all insurance, including cyber insurance, there are two states; a good state and a bad state. Where the bad state is the occurrence of an event causing a loss and negative impact on the wealth of the entity, the good state indicates that there has not been an event leading to a loss of wealth. For our model, we define the probability for a cyber incident leading to a loss of wealth, as "P". Probability "1-P" express the probability that there will not be a cyber incident causing a loss of wealth. During bad state, an entity will lose the difference between the income in good state I(1e) and bad state I(0e), presented by L(e). The amount of coverage is illustrated by S. The premium, which is the $ amount per $ coverage, is illustrated by V*S. The following is the function for measuring the expected utility for cyber insurance.

$$E[U] = p \times U(I_1^e - L^e - \gamma S + S) + (1 - p) * U(I_1^e - \gamma S)$$

(Kuru & Bayraktar, 2017, p. 335; Kesan, Majuca & Yurcik, 2004, p. 8).

5.3.2 Deductible

In the case of insurance for an entity, one must consider the Terms and Conditions presented by the insurance carriers. One of those conditions is the deductible. In the function for the expected utility of business interruption coverage for cyber insurance, we define the deductible as a time retention factor illustrated as Wh. The economic impact of a waiting period on income is calculated by multiplying the relevant waiting period in hours with the hourly cost of the business interruption. The expected utility function for business interruption coverage of cyber insurance is formulated as following:

$$E[U(BI)] = p \times U(I_1^e - L^e - Wh - \gamma S + S) + (1 - p) * U(I_1^e - \gamma S)$$

5.3.3 Expected Utility

Expected utility is an estimate for an entity's sum of utility from its revenue given a set of parameters. Thus, the utility for bad state illustrates the utility an entity will obtain from its revenue given an event leading to a loss of wealth. For good state,

the utility will be the utility of revenue when there is not a event leading to a loss of wealth. The expected utility will be the utility weighted for the probability of a given set of events.

5.3.4 Function Output: The Model

The output of the model is a sum of the expected utility of revenue for the insured entity.
It communicates the difference between sum of expected utility of insurance during bad state, weighted for the probability of a loss event occurring, and the expected utility of insurance during good state weighted for the probability that there will not be a loss event.

We use the following example of expected utility to exemplify the calculation of expected utility of business interruption insurance:

An entity has a utility function U(r) where r (revenue) is the value of production. The entity produces \$1 000 000 in revenue, with a 10% possibility of a fire destroying machinery causing a \$10 000 loss of revenue per hour, the machinery is not replaced before 24 hours after the incident, leading to a 24-hour loss of revenues. The following expected utility when the entity is not insured is:

$$E[U(r)] = Probability \times U(Revenue) + (1 - Probability) \\ * U(Revenue - Fire(loss\ per\ hour) * hours\ of\ interruption)$$

$$E[U(r)] = 90\% \times U(1\ 000\ 000) + 10\% * U(1\ 000\ 000 - 10\ 000 * 24)$$

$$E[U(r)] = 976\ 000$$

The expected utility of revenue given the probability of a fire is 976 000.

If the entity is given the choice of insuring against fire, presuming that the insurance agreement covers an indefinite amount of loss excluding a waiting period of 12 hours for a price (premium) of 10 000. Waiting period of 12 hours, states that the entity must assume the first 12 hours of loss before the insurer becomes liable for the period of restoration and related loss. The following expected utility of an insured entity is then:

$$E[U(r\boldsymbol{i})] = Probability \times U(Revenue - Premium) + (1 - Probability) * U(Revenue - Premium - Fire(loss\ per\ hour) * waiting\ period)$$

$$E[U(r\boldsymbol{i})] = 90\% \times U(1\,000\,000 - 10\,000) + 10\% * U(1\,000\,000 - 10\,000 * 12 - 10\,000)$$

$$E[U(r\boldsymbol{i})] = 978\,000$$

The expected utility of wealth when insured is 978 000.

$E[U(r)]$: $976\,000 < E[U(r\boldsymbol{i})]$: $978\,000$

Based on the theory of expected utility as a tool of ranking the most "choiceworthy" act (Briggs, 2014), the entity will prefer to be insured for business interruption when $E[U(r)] < E[U(r\boldsymbol{i})]$.

5.4 Companies Included in the Model

To be able to create a representative model for the current cyber insurance market, it was necessary to include data from several cyber insurance carriers in the model. The model is therefore based on data from the following carriers of cyber insurance; Berkeley, Chubb, Everest, National State Insurance, Philadelphia, Travelers, and QBE. These seven companies were the only companies with publicly available policies, terms, and rates on SERFF, where the policies available included the possibility to isolate the coverage of business interruption. Thus, it is possible to choose the variables relevant to business interruption and calculate the premium for business interruption coverage on cyber insurance. By including data from these seven cyber insurance providers, we ensure that our data can be generalized for the industry.

5.5 Hazard Classes & Industry Factors

The Hazard class or industry factor is used by most insurance companies to translate information regarding the systematic risks in each industry/profession into a factor influencing the pricing of risk (premium) (IRMI, n.d.a).

5.5.1 Generalizing Hazard Classes

While the price of cyber insurance may share some similarities between the different carriers, the calculation of business and technical factors is quite different (Romanosky et al., 2019). This was further emphasized when designing the model. The insurance carriers used a mix of industry factors with differing factor weightings and hazard class classifications with different ranges. To effectively compare premium prices according to the relevant industries, we had to weigh the different ranges and hazard classes into a range of one to five. Where hazard class one is considered to have the least amount of risk, and hazard class five is considered to have the most risk. The following examples of industries have been found to correspond to the ensuing hazard classes in the underwriting guidelines of the insurance policies.

- Hazard class 1: Construction, Agriculture
- Hazard class 2: Architects & Engineers
- Hazard class 3: Accounting, Technology/Computer consulting, Telecommunication, Manufacturing, Wholesale, Transportation
- Hazard class 4: Healthcare, Utilities, Governmental related, Retail
- Hazard class 5: Stock exchange, Financial firms

5.5.2 Chubb and The Hartford - Industries and Related Hazard Classes

There were two companies, Chubb and The Hartford, which only had defined hazard class range as a factor influencing the pricing of premiums. Without mentioning which industries should be categorized into which hazard class. To be able to employ these companies in the calculation of the premium correctly, we used a weighted average of the industry- and hazard class classification from the insurance carriers, which are already included in the model, Berkeley, State National Insurance (CFC), Philadelphia Insurance, Travelers, and QBE. This results in a classification of industries into hazard classes one to five based on the carriers' average beliefs. The results are further illustrated in table 2 in appendix C1. We conclude that the use of the weighted average does not threaten the internal validity,

given the research of Romanosky et al. (2019) and our own findings of the policies collected, which shows that the insurance carriers share many similarities, especially considering the classification of industry-related cyber risk.

5.6 Estimation of Premium

The model includes data from seven cyber insurance carriers. There is, therefore, a difference in how the different carriers' premiums are constructed and calculated. To ensure that the model is as accurate as possible, it is essential to understand how the differences in premiums between providers can affect the model. Following is a generalization of how the insurance carriers calculate the rates for their policies.

5.6.1 Estimation of Premium for Business Interruption Coverage on Cyber Insurance

The carriers have different procedures to calculate premiums; even so, there are some similarities in the process. These similarities are the following core operations of the calculation of premiums. They will first establish a base rate; this includes classifying a rate to a given revenue or revenue band. Next is the increased limit factors (ILFs). The ILFs are the factors that allow for an increase or decrease in the coverage limit. Following the ILFs is the industry factor, which also is defined in some cases as the hazard class factor. Industry factors take into consideration the systematic risks related to the industries.

Whereas the hazard class factors group different industries into different hazard classes, which implicitly takes into consideration these risks just grouped. Further, the estimation includes the schedule rating. The schedule rating adjusts the premium for different entity-specific risks, such as their security systems and procedures during and after an event. The last factor is the retention factor, also called the waiting period for business interruption coverage. The waiting period factor is the time before the period of restoration will initiate.

5.6.2 Differences in Premium between Carriers

The premiums calculated show differences between the carriers**.** The most distinct characteristic of the premiums, which should be noted, is that the premium prices converge towards each other when the waiting period is increasing, as illustrated in figure 3.

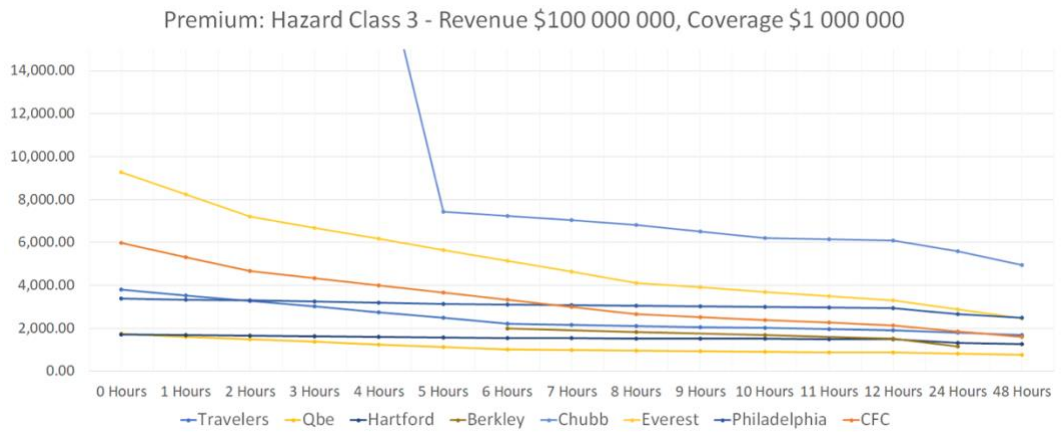


Figure 3

This graph illustrates the premium prices offered by the seven insurance carriers for an entity in hazard class three, with a revenue of $100 000 000 and insurance coverage of $1 000 000.

5.6.3 Calculation of Premium - Omitting Values

To ensure that the data used in the model is adequately representing the whole industry, and not only the beliefs and rates of one company, we chose to use the average premium of five of the companies which were found to be relevant. Chubb's data was omitted, as the premiums for waiting periods from six hours and towards zero grew exponential and were high enough to be considered as an extreme outlier, this can be observed in figure 3**.** The data from Berkley was also omitted. Berkley did not state the possibility to use linear interpolation to calculate missing factors. Thus, we could only under reasonable assumptions calculate premiums for six-, eight-, ten-, twelve-, and 24-hour premiums. Since a premium for each hour from zero to twelve, 24, and 48 hours was needed, we excluded Berkley.

5.7 Loss Function

We chose a linear loss function of cyber attacks for our model. This was done due to the lack of accurate data, methods of estimating cyber risk, and the complex estimation of business interruption (Schumann, 2013). As cyber insurance is a relatively new and immature product and risk, the linear loss function is derived using the revenue as a base. By dividing the base by 365 (days) and then 24 (hours), it results in the hourly loss of a cyber event.

5.7.1 Hazard Class-Specific Loss Factor

The core calculation of loss would have been adequate for the model if all insured entities had the potential for identical losses if all else were equal. This, however, is not the case based on the revenue operations of each industry. In an effort to adjust the model for the industry-specific conditions, we add hazard class-specific loss factor to the linear cost model. This factor is meant to adjust for the difference in loss between the hazard classes. As OECD (2017) elaborated, there is a concern in the insurance market on how to quantify the risk of cyber attacks. Following this, there is no publicly available data on the losses of a cyber incident and how the losses may differ based on the industry classification of the affected company. We therefore propose, and use the following linear factor for each of the hazard classes in our model;

- Hazard class 1: 0.8
- Hazard class 2: 0.9
- Hazard class 3: 1
- Hazard class 4: 1.1
- Hazard class 5: 1.2

5.8 Assumptions

5.8.1 Entity Parameters

To be able to accurately compute, compare, and summarize the premiums from the selected rate calculations, we had to assume that the computed premium, based on the theoretical entity, was performing "averagely" on the parameters set for rate calculation. This presumes that the entity is performing average on parameters such as IT-security, breach plans, storage of confidential information, and so on. Average performance will be indicated in the premium calculation as a factor equal to one, and therefore, not have an impact on the calculation of premiums. The notion that a factor equal to one neither has a positive or negative effect is highlighted by Travelers Insurance underwriting guidelines, stating that "In the event sufficient information is not available to allow for an assessment and evaluation of the underwriting risk imposed by any applicable rating factor, a neutral factor (1.00) will apply for such a rating factor." (Travelers, 2020).

5.8.2 Linear Interpolation

When designing an insurance policy for an entity, the insurance carrier may leave room for flexibility. To be able to leave room for the underwriter to assess the risks accurately without creating a large dataset, the insurance carriers establish the possibility of applying linear interpolation for missing values. Linear interpolation is a method of estimating a value c by observing two data points (a, b). These two data points are then used to construct a linear function finding the approximate value of c as a value between a and b. We applied linear interpolation on the insurance carriers' rates to find several of the missing values for the waiting period parameter.

5.8.3 Hazard Class

We assume that the industry has an overall understanding of the systematic risk of each industry and will classify each industry into appropriate hazard classes. This assumption was used when deriving the average weighted hazard class for The Hartford and Chubb and is further supported by our findings in insurance policies, underwriting guidelines and interviews with industry professionals.

5.9 Limitations

5.9.1 Missing Data

Our research method is based on publicly available information. This means that we have only taken into account policies and rate schedules, which are submitted as part of the admitted market. Carriers that operate in the admitted market in the U.S. must file their policies and following rate schedules with their state insurance commissions. To be able to offer insurance to admitted markets, the insurance carrier must be licensed by the state commissioners. Non-admitted carriers, which are also referenced to as surplus/excess lines are unlicensed, therefore, they are not backed by the state department of insurance and thus do not operate under the same strict regulations as admitted carriers (Insureon, 2018; NAIC, 2019). Some argue that the majority of cyber insurance policies is written in the non-admitted market (Greenwald, 2016).

According to NAIC (2019) report on "Cybersecurity insurance and Identity Theft coverage", the total U.S. market for cyber insurance was approximately $3.6 billion. Of this, there were $2.03 billion direct written premiums in the admitted market. This indicates that there were approximately $1.57 billion written premiums in the non-admitted market. The non-admitted carriers do not have to submit their policies

or rate schedules to the state insurance commissioners (Romanosky et al. 2019, p.3). Hence the missing data on premiums from the non-admitted carriers may limit our study and external validity.

5.10 Approximation

5.10.1 Average

By using averages, we enable a more comprehensive and objective perspective. While averages allow for a general approach and takes several sources into consideration, the average is sensitive to extreme and "heavy-weighting" values. To offset the extreme values, we have omitted one insurance carrier, Chubb, due to their extreme values for some specific intervals of waiting period.

5.11 Simplification

5.11.1 Simple Function

To compare the return on each level of waiting period, we had to find a "simple"-function. The function had to allow for flexibility, but still have the ability to generalize the results. Hence, we decided on an expected utility function. While the expected utility function may lack an absolute ability to be adopted in the real world based on the theoretical nature of utility. We see that the expected utility function will express which parameters will indicate, within reasonable boundaries, the optimal choice for a given entity. The application of a "simple" function may not completely illustrate complex situations for an insured entity. However, under current circumstances, it may be what is possible, considering the complicated and comprehensive nature of cyber risk and insurance-related calculations.

5.11.2 Linear Loss-Function

Calculating costs and implications related to physical business interruption is a complicated procedure (Schumann, 2013; Deloitte, 2016). Applying business interruption to cyber insurance involves adding a whole new layer of complexity regarding cyber risk, comprehensiveness, and uncertainty (Cohen, n.d). Therefore, we had to limit the estimation of loss to a linear loss-function.

5.12 Trade-Offs

One of the limitations threatening further adaptability is the geographical limitations that are imposed as a result of the particular source and collection of data. To be able to find a data fundament for our analysis we had to limit the thesis to the admitted insurance carriers and their submitted cyber insurance policies in the U.S. This may be disadvantageous for further global adaptability of the study, due to the different regulations, restrictions, and attributes of other insurance markets.

5.13 Our Comments

The insurance industry is a complicated industry with many different actors. Where the insurers provide the same type of insurance, their terms and definitions often vary. This may be explained by the insurers' history and roots, for example, starting out with a specific type of insurance, originating from different continents or different countries. Thus, they have developed their own way of constructing policies, with different definitions, terminology, limits endorsements, exclusions, etc. This makes it more complicated to develop a model, as there is often insufficient clarity on what is covered and what is excluded between different carriers.

For the model and following results, we don't take into account the acquiring costs of insurance and whether the insured is risk-averse. That is when the entity will prefer to be insured and pay a fixed fee, instead of facing exposure to an arbitrary amount. The acquiring costs of insurance can be costs related to insurance brokers and costs associated with due diligence.

5.14 The Chosen Parameters

For our estimation of expected utility, we set the following parameters:

5.14.1 Probability

Because of the intricate and continuously evolving nature of cyber risk, it is extremely difficult to set factual probabilities for events occurring. This is due to aspects of estimating the likelihood of cyber risk, such as the lack of publicly available data and complexity involving estimation of risk, which is supported by

ENISA et al.'s (2012) and OECD's (2017) analysis of the current situation in the cyber insurance market. We propose the following probabilities to illustrate different scenarios;

- 1.0%, 5.0%, and 10.0%

5.14.2 Revenue

To analyze entities in different scenarios and how premium may differ between them, we categorize the entities' revenue as follows:

- In $ millions, 50, 100, 250, 500, 1000.

5.14.3 Length of Attack

Gerking and Smith (2017) found that the most significant DDoS attack to have hit a U.S. company was fully resolved within 11 hours, thus supporting the need for short(er) waiting periods. The Ponemon Institute (2012), found that the average amount of downtime due to an DDoS was 54 minutes, which is in accordance with the findings of Gerking and Smith. Regarding the short duration of many cyber incidents, we choose the following lengths of attack to analyze:

- In hours, 4, 8, 12, 18, 24, and 48.

The Ponemon Institute illustrated their findings as follows:

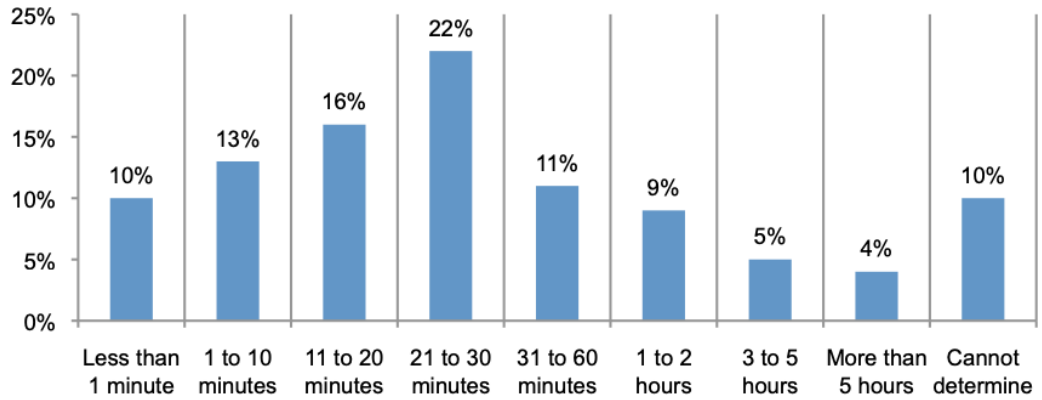


Figure 4 - Average downtime after one DDoS attack

(Ponemon Institute & Radware, 2012, p.6).

5.14.4 Waiting Period

For our model we have chosen the following waiting periods;

- Zero to twelve hours, 24 hours, and 48 hours.

These waiting periods may, in the perspective of traditional insurance policies, be regarded as short, where waiting periods usually start at 12 hours and in some

policies can be several months. The reason to only include relative short waiting periods in the model is due to the nature of cyber incidents where the incidents often are resolved well within the first 12 hours (Gerking & Smith, 2017, p.17; The Ponemon Institute, 2012). This can also be illustrated by the cyber attack on Dyn's servers, which caused an estimated $110 million in business interruption losses. Due to the long waiting period used, little of the losses were covered since these were longer than the disruption caused by the DDoS (OECD, 2017, p. 37).

Among the insurance carriers, we observed the possibility of selecting waiting periods between 0-168+ hours, depending on their provisions. Furthermore, we found that an 8-hour waiting period returned a time retention factor of 1.00 for most of the insurance carriers (Everest, State National Insurance, Travelers, and QBE). For Chubb, the standard waiting period was 10 hours and for Philadelphia Insurance, Berkley Insurance, and The Hartford, it was 12 hours. Since we omit Chubb and Berkley from the model, we assume that the standard waiting period of the relevant carriers and thus, the industry is 8 hours. (Berkley, 2018; Chubb, 2019; Everest, 2019; Philadelphia, 2019; QBE, 2019; State National Insurance, 2019; The Hartford, 2020; Travelers, 2020)

Coverage

We decided to include five different coverages in the model, ranging from $1 000 000 to $5 000 000, since we recognize that $1 000 000 in coverage may not accommodate all revenue ranges.

5.15 Hypotheses

The following hypotheses were derived from the research question, to categorize and test the results.

Hypothesis 1:

- **H0:** There is no prominent choice of waiting period; the expected utility is relatively static for increased or decreased values of time retention.
- **H1:** There is a choice of waiting period, which particularly returns a higher positive expected utility than the other waiting period levels.

Hypothesis 2:

- **H0:** There is no- or negative return on choosing a waiting period, which is shorter than the industry standard (8 hours).
- **H1:** There is a positive return on the expected utility of choosing a waiting period, which is shorter than the industry standard (8 Hours).

Hypothesis 3:

- **H0:** Choosing a waiting period of 0 hour will not achieve the highest positive expected utility.
- **H1:** Choosing a waiting period of 0 hour will achieve the highest positive expected utility.

6 Results

We find that there is a choice of waiting period, which particularly returns a positive expected utility, but this depends on the probability of attack. Further, we want to focus predominantly on 4-, 8-, 12-, 18-, and 24 hours of incident, due to the circumstances and characteristics of cyber incidents and our research question. While we find an incident length of 48 hours interesting, this doesn't fully fit into the short durations of cyber incidents. However, a 48-hour incident length returns positive expected utility for all values.

In the results, when we refer to optimal coverage, we refer to the situation where an entity chooses the coverage which maximizes its expected utility. This we define as the equilibrium between coverage versus loss and the premium, resulting in the highest expected utility for a given incident length and revenue.

To be able to illustrate how the different hypotheses are affected, we categorize the results into the three probabilities in the model and test the hypotheses for each of the probabilities.

6.1 Results of Hypotheses

6.1.1 Results for 10% Probability

Hypothesis 1

We observe that at a 10% probability of a cyber incident, for all cyber incident lengths, there is positive expected utility, expect at an incident length of 4 hours and $50 000 000 revenue. This implies that an entity will insure in almost all cases, regardless of revenue and hazard class. Or for every expected length of cyber incidents except 4 hours. For all lengths, given that there is optimal coverage, the highest expected utility is at a 0-hour waiting period. We can, therefore, reject hypothesis 1 for all values expect at revenue $50 000 000 at an incident length of 4 hours and conclude that there is a prominent level of waiting period in which an entity should choose to maximize its utility level.

Hypothesis 2

Following this, we can reject hypothesis 2 and conclude that there is a choice of waiting period, which will return a positive expected utility for waiting periods shorter than 8 hours for all values, which rejects hypothesis 1.

Hypothesis 3

We observed that all values which reject hypothesis 2 would return the highest positive expected utility at a 0-hour waiting period. Therefore, we can reject the null hypothesis of hypothesis 3, and conclude that choosing a 0-hour waiting period will maximize the expected utility of an insured entity.

6.1.2 Results for 5% Probability

Hypothesis 1

We observe for a 5% probability that most of the values are positive except for all values at a revenue of $50 000 000, for incident lengths of 4- and 8 hours. And at a $100 000 000 revenue for an incident length of 4- and 8 hours for hazard class 5. Therefore, we can conclude that the null hypothesis of hypothesis 1 can be rejected for all values except for revenue $50 000 000 at 4- and 8 hours length for all hazard

classes and for revenue $100 000 000 at an incident length of 4 hours for all hazard classes, and 8 hours for hazard class 5.

Hypothesis 2

Given that there is an optimal coverage, for every value which rejects hypothesis 1, we find that they also reject hypothesis 2. Every value that has a positive expected utility reflects that a 0-hour waiting period will return the highest expected utility, which is shorter than what we have concluded to be the industry standard (8 hours).

Hypothesis 3

As stated in the results of hypothesis 2 for 5% probability of an incident, every value which has a positive expected utility will return the highest expected utility at a 0-hour waiting period. Thus, concluding that we have to reject the null hypothesis of hypothesis 3, and state that a 0-hour waiting period will return the highest expected utility.

6.1.3 Results for 1% Probability

Hypothesis 1

We find that the lower range of revenues, i.e., $50 000 000 and $100 000 000, will return negative expected utility for all hazard classes at all incident lengths. Thus, for all revenues equal to or below $100 000 000, we must keep the null hypothesis of hypothesis 1.

We observe that for $250 000 000 revenue, only a few incident lengths will contribute to a positive expected utility. That is, for all hazard classes except hazard class 1, it is negative for 4-, 8-, 12- and 18-hours incident lengths. While for hazard class 1, it is positive for incident lengths of 18- and 24 hours. We can conclude that the null hypothesis of hypothesis 1 can only be rejected for some values of incident length when an entity has $250 000 000 in revenue.

At revenue of $500 000 000, there is positive expected utility at incident lengths of 18- and 24 hours for all hazard classes. Thus, we can reject the null hypothesis of

hypothesis 1 for a revenue of $500 000 000 at an incident length higher than 18 hours.

For revenue $1 000 000 000, there is a positive expected utility for incident lengths of 12-, 18-, and 24 hours. Thus, we can reject the null hypothesis for hypothesis 1 for a revenue of $1 000 000 000 at lengths above 12 hours.

Hypothesis 2

Following, we will conclude whether the values which rejected the null hypothesis of hypothesis 1, can reject the null hypothesis of hypothesis 2.

We observe that for a revenue of $250 000 000, it is only the incident length of 18 hours for hazard class 1, and 24 hours for the remaining hazard classes which rejects the null hypothesis of hypothesis 1. For an 18-hour incident length, we find the highest expected utility to be at a 2-hour waiting period for hazard class 1. At an incident length of 24 hours, we have the highest expected utility at a 2-hour waiting period for hazard classes 1, 2, and 5, while for hazard classes 3 and 4, it is at a 6-hour waiting period. Thus, we can reject the null hypothesis of hypothesis 2 for all values which have a positive expected utility.

For a revenue of $500 000 000, we find that for an incident length of 18 hours, the highest expected utility is at a 2-hour waiting period for hazard classes 1, 2, 3, and 4, while at a 4-hour waiting period for hazard class 5. At an incident length of 24 hours, the highest expected utility is at a 2-hour waiting period for hazard class 1, at a 5-hour waiting period for hazard class 2, at a 6-hour waiting period for hazard class 3, at an 8-hour waiting period for hazard class 4, and at a 9-hour waiting period for hazard class 5.

As a conclusion, the null hypothesis of hypothesis 2 can be rejected when the incident lengths are 18 hours for all hazard classes. We find that at an incident length of 24 hours, the null hypothesis can only be rejected for hazard classes 1, 2, and 3. For hazard classes 4 and 5 at a 24-hour incident length, the null hypothesis holds.

At a revenue of $1 000 000 000, we observe that for an incident length of 12 hours the highest expected utility is at a 1-hour waiting period for hazard class 1, at a 2-hour waiting period for hazard class 2, at a 3-hour waiting period for hazard class 3, at a 4-hour waiting period for hazard class 4, and at a 5-hour waiting period for hazard class 5.

For hazard class 1 at an incident length of 18 hours, the highest expected utility is at a waiting period of 2 hours. The highest expected utility is at a 2-hour waiting period for hazard class 2. For hazard class 3, it is at an 18-hours incident length, and the highest expected utility can be found at a 9-hour waiting period. The highest expected utility for hazard classes, 4 and 5, is at a 10-hour waiting period.

For 24 hours of incident length, we find the highest expected utility for all hazard classes at a coverage of $2 000 000.
The highest expected utility for hazard class 1 is at a 2-hour waiting period. The highest expected utility for hazard class 2 is at a 24-hour incident length and a 5-hour waiting period. For hazard class 3, the highest expected utility is generated at a 7-hour waiting period. Hazard class 4 maximize its expected utility at a 24-hour incident length with an 8-hour waiting period. Lastly, hazard class 5 will generate the highest expected utility at a 9-hour waiting period for an incident length of 24 hours.
We find that all maximizing levels of a waiting period in an incident lasting 12 hours are below 8 hours; hence we can reject the null hypothesis of hypothesis 2. For an incident lasting 18 hours, we can only reject the null hypothesis for hazard class 1; thus, we have to keep the null hypothesis for hazard class 2-5. At an incident length of 24 hours, we can reject the null hypothesis for hazard classes 1- 3, while keeping the null hypothesis for hazard classes 4 and 5.
Hypothesis 3
As observed previously for hypothesis 2 at 1% probability, there are no values that can reject the null hypothesis for hypothesis 3, hence concluding that choosing a 0-hour waiting period will not maximize the expected utility for an entity with revenue between $50 000 000 and $1 000 000 000.

6.1.4 Summary of the Results of the Hypothesis Testing

For the probabilities 10% and 5%, hypotheses 1, 2, and 3 will be rejected for almost all values, except some values at an incident length of 4 hours. Concluding that for these positive probabilities, an entity will achieve the highest expected utility when choosing to insure, and at a 0-hour waiting period.

The results are more heterogeneous for a probability of 1%, thus illustrating several distinct trends. Hypothesis 1 holds for revenues equal to or below $100 000 000 and most values related to revenue of $250 000 000. This indicates that entities with revenues equal to $250 000 000 or below, in most cases, should not insure, since this will provide a negative expected utility. Furthermore, hypothesis 2 holds for some values, which imply that there are some values where a utility-maximizing entity should choose a waiting period, which is less than 8 hours. The most significant findings are that there are no values where hypothesis 3 will be rejected. Hence, we can conclude that an entity for any given value within the chosen parameters and 1% probability will not maximize its expected utility choosing a waiting period of 0 hours.

7 Discussion

In the following discussion, we will focus primarily on the values related to the 1% probability of an incident, although we will comment briefly on probabilities of 10% and 5%. This is due to two reasons.

The first is the applicability to reality, i.e., we see that the 1% probability is the one probability out of the three analyzed which reflects real conditions the most. The second reason is the heterogeneity of the results. For 10% and 5%, we observed that the results were mostly homogenous, referring to that essentially, all results were positive and returned the highest expected utility at a 0-hour waiting period. We see this as a result of the impact on expected utility by a cyber incident, when the probability rises; thus, the influence of the loss rises disproportionally related to the weighted premium.

This is also observed for incident lengths of 48 hours, therefore, it is plausible for longer lengths too. There is positive expected utility for at least one level of waiting

period for approximately all revenues and hazard classes regardless of probability. This suggests that if there is probable that incidents lengths will be equal to or longer than 48 hours, entities will choose to insure as there is positive expected utility related to the waiting period levels.

7.1 Higher Levels of Probability

To establish a context, we will elaborate on some trends we find interesting for the higher levels of probabilities, i.e., 10% and 5%. For higher probabilities, we found that for optimal coverage, approximately all values were positive and the expected utility would increase towards and culminate at a 0-hour waiting period. When the probability of an incident is high, the impact of loss is significant enough that an entity optimizes its utility by choosing the lowest waiting period. The trend of increasing expected utility for lower waiting periods reinforces the initial thought that the current standards of cyber-related business insurance terms. Referring to waiting period, it is not adequately fitted to the properties of cyber risk. Entities exposed to higher probabilities, i.e., at least 5% or higher, should, therefore, insure for cyber-related business interruption and decide for the lowest waiting period possible.

High Probabilities Equal High Risk

While this may be optimal theoretical, the practical applicability may be low. This may be due to the adverse situation of an entity facing high probabilities of a cyber incident. Several insurers provide precautions in their underwriting guidelines about providing insurance for high-risk entities, such as government-related entities and large-scale data aggregators. This may result in insurance carriers either offering standard or sub-optimal terms or deciding not to insure the entity at all. Entities exposed to high probabilities of incident should, therefore, choose to insure at a 0-hour waiting period. This maximizes their expected utility, given that their present conditions allow it. The expected utility for an entity with a revenue of $250 000 000 is illustrated in figure 5. In fact, the highest expected utility at a 0-hour waiting period is occurring for approximately all values of revenue, which rejects hypothesis 1 for probability equal to or larger than 5%.

In the present-day market conditions, entities may find it complicated to obtain a 0-hour waiting period as insurance carriers will refrain from writing cyber related

business interruption coverage with a short waiting period. Following interviews with industry professionals and underwriting guidelines, carriers may refrain from writing insurance with waiting periods lower than or between 4 and 6 hours.

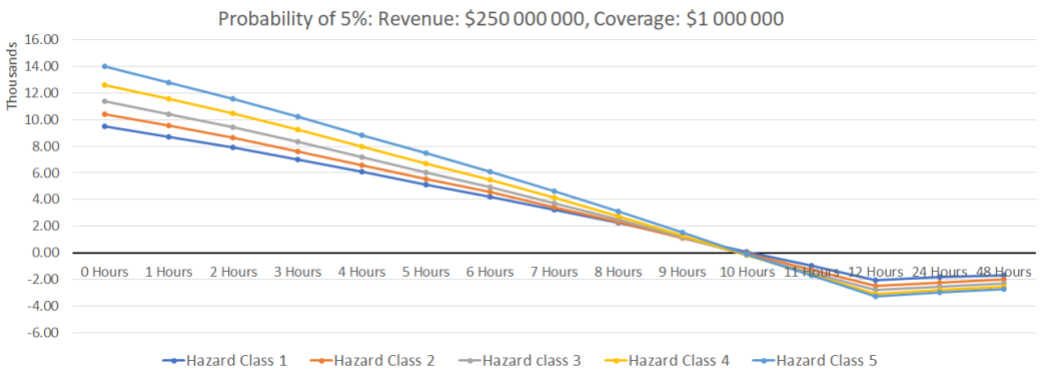


Figure 5

Optimal Coverage

We also observed for probabilities equal to, or higher than, 5%, that there is not a coverage that is optimal for all revenues. This is noted by the following graph illustrating total costs for a given incident length, where the dotted line illustrates a coverage of $1 000 000.

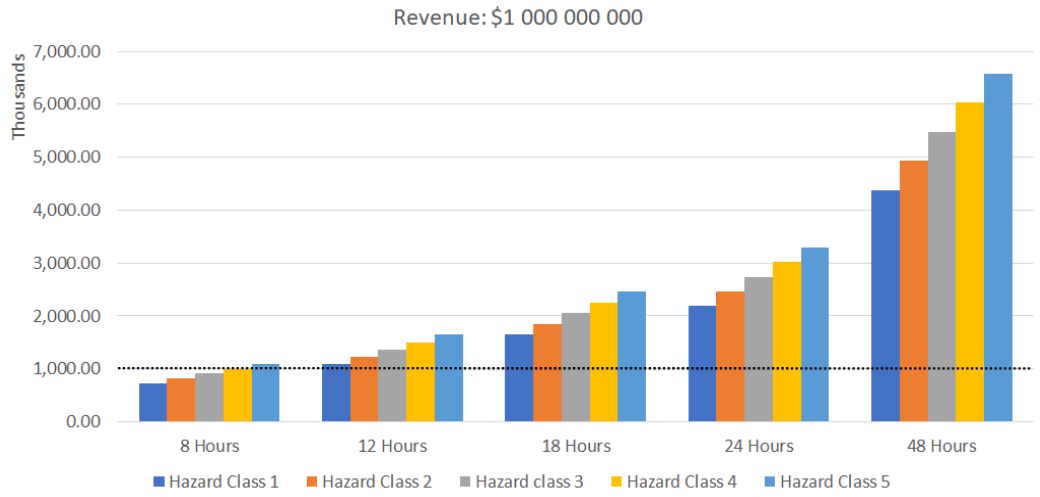


Figure 6

As stated in relevant literature, sub-optimal coverage is one of the effects of the immature cyber insurance market (CISA, 2019). This statement is further supported by Unhammer (personal communication, February 4, 2020), which elaborated that one of the substantial pitfalls of companies choosing to insure against cyber risk is

to not have sufficient coverage. This was further emphasized by CISA in their report on cyber insurance from 2019, and the data analyzed in this thesis. It was found that insuring may return a positive expected utility, but an entity will not achieve the maximum expected utility, unless choosing optimal coverage. Illustrated in figure 7 is how the maximized expected utility will differ when taken into consideration different levels of coverage for an entity with revenue of $1 000 000 000, exposed to a 5% incident probability and an incident length of 24 hours.

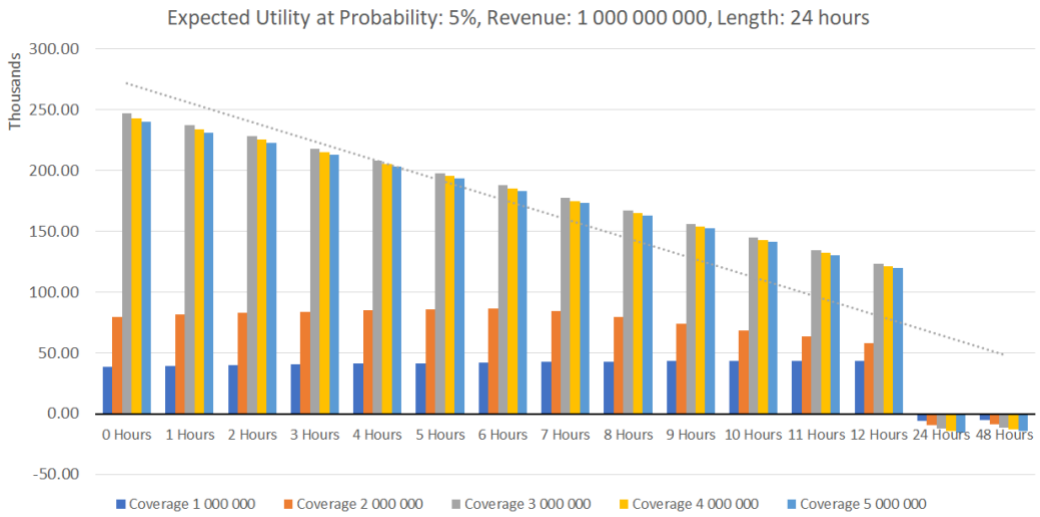


Figure 7

As emphasized by the trend lines, the highest expected utility levels will shift related to different coverages. We can derive that for this scenario, an entity will achieve the highest expected utility at a coverage of $3 000 000, illustrated by the grey color. This leads us to conclude that an entity will choose the optimal coverage related to their revenue and perception of potential incident length. To be able to maximize their expected utility and rationally choose a 0-hour waiting period. Thus, supporting our findings in relation to hypothesis 3.

Conclusion for Higher Probabilities

For probabilities higher or equal to 5%, the expected utility is positive for approximately all values except for lower revenues at a 4-hour incident length. At optimal coverage, the highest expected utility for all revenues is at a 0-hour waiting period. However, it may be challenging for an entity to acquire terms with a 0-hour waiting period, due to the entity being exposed to high risks and potential for significant losses. It also raises the question of whether an entity will be able to choose the optimal coverage.

7.2 Lower Level of Probability

Opposed to higher levels of probabilities, an entity will achieve higher expected utility at a coverage, which is less than the loss at a 1% probability of an incident. This indicates that an entity will have a positive return when self-insuring a piece of the loss. Self-insuring is when an entity decides to retain some or all risk.

7.2.1 Revenues Smaller or Equal to $100 000 000

The calculations show that for all hazard classes, the lower range of revenues i.e., $50 000 000 and $100 000 000, will return negative expected utility at all relevant lengths of incident. This tells us that theoretical entities which have revenues equal to or below $100 000 000 should not insure on account of their return on expected utility. Literature and empirical data state that for SMEs hit by a cyber incident, there is a considerable probability of filing for bankruptcy or going out of business (National Cyber Security Alliance, 2019). Vintage, Cisco, and NCMM (2018) finds that up towards 60% of SMEs go out of business six months after being subject to a successful cyber attack. They are thus affirming the importance of having a viable tool to mitigate the impact of cyber incidents.

Nascent SMEs Market

The notion that SMEs have a considerable need for cyber insurance contradicts our findings that entities with lower ranges of revenues should not insure. Our findings on expected utility may be skewed by the development of the insurance market. We have previously, through findings in literature and interviews with industry professionals, noted that the cyber insurance market for SMEs is underdeveloped. This may influence the underwriting of risk and, in turn, premiums. Further questioned is whether the coverage may be sub-optimal for smaller entities; this is illustrated in the following graph for an entity with revenue of $100 000 000. Coverage of $1 000 000 is too high relative to the expected losses even for an incident with lengths upwards to 48 hours. Considering the possible short durations of cyber incidents, optimal coverage may be lower than $1 000 000. As follows for all the insurance carriers' rate schedules, reduced coverage will reduce the premium. Concluding that optimizing coverage may shift cyber-related business interruption coverage for SMEs to a positive expected utility. Illustrated in figure 8 is the aggregated loss for each hazard class at each incident length.

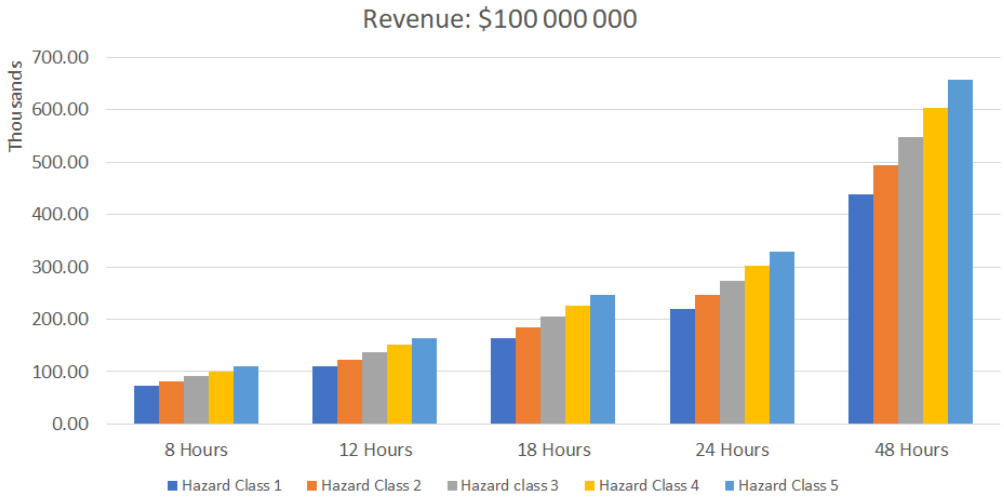


Figure 8

7.2.2 Revenue Greater than $250 000 000

The expected utility shifts from negative to positive from revenues of $250 000 000 and upwards at certain lengths of waiting periods and incident lengths. However, this is only at an 18-hour incident length for hazard class 1 and at an incident length of 24 hours for the remaining hazard classes. This implies that an entity with a revenue of $250 000 000 should only insure if it's exposed to incidents with a 1% probability and incident lengths equal to or higher than 24 hours (or an 18-hour incident length, for hazard class 1). When the revenue increase from $250 000 000 and up to $1 000 000 000, the expected utility will increase, shifting values from negative to positive for incident lengths shorter than or equal to 18 hours. This can be observed for hazard class 2, at a coverage of $1 000 000 and an incident length of 18 hours, as illustrated in figure 9. Higher revenue will increase the expected utility, which implies that entities with higher revenue will be more inclined to insure, assuming that the entity bases their decision upon expected utility.

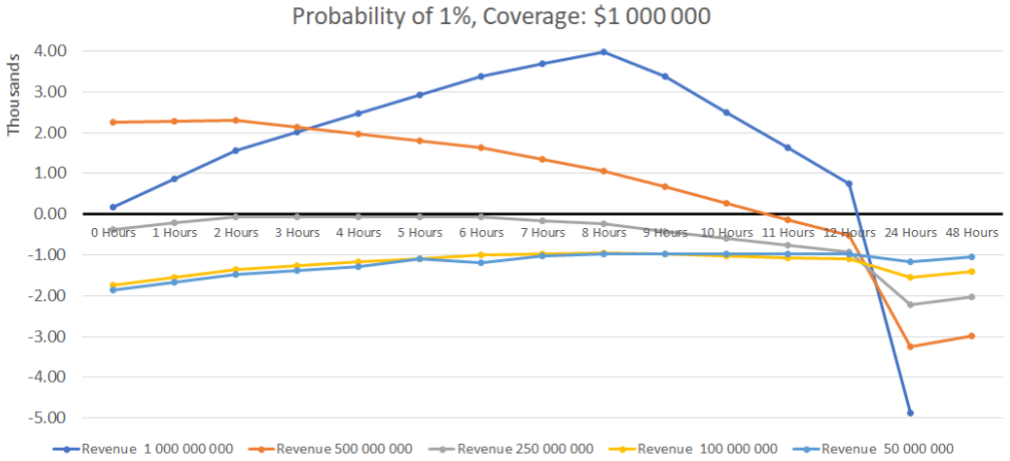


Figure 9

This is further supported by our interviews with industry professionals and relevant literature, which states that larger companies are more inclined to insure for cyber exposure. It is also clear that adoption and market penetration of cyber insurance is substantially higher for large corporations than for SMEs. Ingebrigtsen and Unhammer comment further that large corporations often have more professionalized risk assessment routines and more comprehensive IT-departments, which will help decrease the potential risk of incidents. This, in turn, may decrease the premiums and thus increase the expected utility.

Increasing waiting periods for revenue and hazard classes

The disproportionate relationship between premiums, revenues, and costs may be what is causing that for higher revenues; the waiting period will increase for identical parameters. As illustrated in figure 11 and table 3 in the appendix. The waiting period, which returns the highest expected utility, will increase for higher revenues. What is further worth noticing in figure 10, is that for a given incident length and revenue, the optimal waiting period will increase per hazard class. That is, if an entity with revenue of $500 000 000 classified as hazard class 1 is exposed to a 24-hour incident length, it will choose a waiting period of 2 hours. While an entity with identical revenue, but classified as hazard class 4, will choose a waiting period of 8 hours. Hence, we can conclude that entities in higher hazard classes will prefer longer waiting periods.

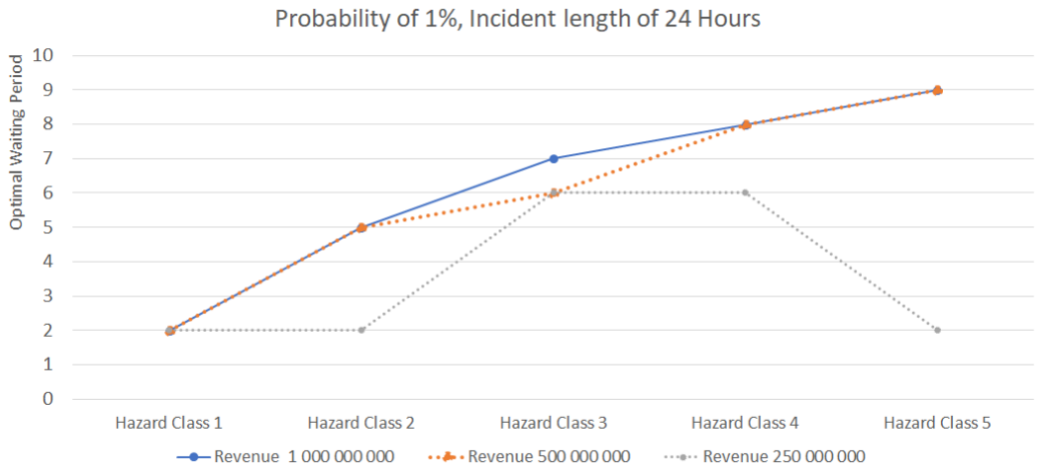


Figure 10

Higher hazard classes may prefer longer waiting periods because the risk associated with an entity increases when the hazard classes shift upward, and the premium will then increase. Another reason why the waiting period increases, may be due to the increased expected utility when entities opt to self-insure. As the marginal utility of covering one extra hour of loss decrease in relation to the marginal increase in premium per extra hour of waiting period. Therefore, an entity will choose to self-insure for a certain amount to attain the highest expected utility possible, given its circumstances and hazard class.

Four- and eight hours of incident length

The length of cyber incidents could be quite short; this is demonstrated in figure 4 by Ponemon Institute & Radware (2012). This leads to the need to consider incident lengths of 4- and 8 hours. At an incident length of 4- and 8 hours, there is no set of values for either revenue or hazard class, which returns a positive expected utility. This may imply that the cyber-related business interruption is still underdeveloped and not optimized, such as Gerking & Smith (2017) described. Hiscox's (2019) survey found that 15% of all the incidents that have occurred were DDoS-Attacks and the Ponemon Institute (2012) found that DDoS-attacks have an average downtime of 54 minutes. This empirical data demonstrates the need for cyber-related business interruption coverage to include shorter waiting periods; this is supported by Gerking & Smith (2017). Concluding that cyber-related business interruption is not adequately adapted and optimized for entities in need of insuring against threats equal to or shorter than an incident length of 8 hours.

Zero waiting period

What is interesting for a probability equal or lower than 1% is that there is no set of values that returns the highest positive expected utility at a waiting period of 0 hours. When decreasing the length of waiting period, the premium will increase. Consequently, a 0-hour waiting period requires a considerable premium. The marginal increase in expected utility of one extra hour of covering losses is not substantial enough to outweigh the marginal decrease of expected utility due to the increased premium. Therefore, we can conclude that the optimal choice of waiting period is higher than 0 hours and may also be equal to or above the industry standard of an 8-hour waiting period.

Optimal Waiting Period

As noted earlier, the waiting period returning the highest expected utility will increase for higher revenues, given that other parameters are identical, this is illustrated in table 3 in the appendix C1. The waiting period returning the highest expected utility will also increase when the incident length increases. Explanations to this can be that self-insurance is a preferred choice when facing adverse infrequent cyber incidents, or that the premium cannot be justified in relation to the possibility of loss.

This gives, that for a shorter incident length, a lower waiting period should be chosen to achieve the highest expected utility. As an example, an entity classified as hazard class 3 with a revenue of $1 000 000 000, should decide for a 3-hour waiting period, given an incident length of 12 hours. It should choose an 8-hour waiting period if the incident length is 18 hours, and it should choose a 7-hour waiting period if the incident length is 24 hours.

While we find that there exists an optimal level of time retention, the optimal level will differ between different incident lengths, further complicating a hypothetical decision process for an entity. Considering the relatively short duration of cyber incidents, an incident length of 12 hours may be what is most representative for an entity exposed to cyber risk. Concluding that for the highest revenue, i.e., $1 000 000 000, an entity should choose a waiting period lower or equal to 5 hours for all hazard classes under the prevailing conditions in the current insurance market.

At an incident length of 18 hours and 24 hours, the optimal waiting period will be higher than for a 12-hour long incident. For revenue of $1 000 000 000, the optimal waiting period for hazard class 3, 4, and 5 is respectively 8-, 10- and 10 hours. This demonstrates that at these incident lengths, standard waiting periods may be the best fit. However, this may be skewed as cyber policies are designed for larger entities, hence the premiums are designed to fit these levels.

For lower levels of revenue, i.e., $250 000 000 and $500 000 000, as previously discussed, there is no positive values for expected utility at incident lengths of 12 hours. This implies that the cyber-related business interruption coverage is not designed for shorter lengths of incidents. For revenue of $500 000 000, it is

observed that for an incident length of 18 hours, the highest expected utility for all hazard classes is at a waiting period equal to or shorter than 4 hours. For revenue $250 000 000, there are only positive values for hazard class 1, at a 2-hour waiting period. This shows that there are still several negative values for shorter incidents and lower revenues, further supporting the notion that the cyber-related business interruption coverage is immature when confronted with the short duration of cyber risk and the needs of the insured entities. Whereas cyber insurance may be underdeveloped, the present values indicate that for an entity to maximize its expected utility, the entity should choose waiting periods shorter than the industry average of 8 hours, when exposed to incidents shorter than 18 hours.

The findings in relation to waiting periods is that cyber insurance products are still immature. However for the conditions at the present time and based on the utility theorem, an entity with revenue equal to or lower than $500 000 000, should for shorter incidents such as incident lengths equal to or shorter than 18 hours, choose waiting periods which are equal to or shorter than 4 hours, converging towards 2 hours. For incident lengths longer than 18 hours, an entity should choose a waiting period longer than 4 hours. For incident lengths equal to or longer than 24 hours, higher hazard classes (4 and 5) at revenues of $500 000 000 should choose a waiting period, longer or equal to 8 hours. At revenues of $1 000 000 000, an entity should choose a 5 hour or shorter waiting period given an incident length of 12 hours.
The optimal waiting period increases towards a 10-hour waiting period for hazard classes 3- 5 at an incident length of 18 hours.

For hazard classes 3-5, the optimal waiting period stabilizes at around 7-9 hours of waiting period for an incident length of 24 hours. While an entity classified as a lower hazard class, i.e., 1 and 2, should choose a 2-hour waiting period at an incident length of 18 hours. For an incident length equal to 24 hours, entities in hazard class 1 and 2 should choose a waiting period of 2- and 5 hours, respectively.

Positive return even at negative expected utility.

The analysis finds that there is not a positive return on expected utility when insuring at lower range of revenue or for shorter incident lengths. While this may be theoretically supported by utility theory, the individual preferences of the specific entity are not considered. A unique preference could be an inclination to

insure due to risk aversion, where the entity prefers to pay a fixed amount instead of being exposed to an arbitrary loss. Insurance may also be a component in a risk management strategy, indicating that the insurance's expected utility may be negative when isolated, but shift to a positive value when taken into account the remaining risk management components. Also, the aggregated expected utility may differ from the individual expected utility for each incident, possibly returning positive expected utility when taken into consideration that there may occur several incidents with different lengths and losses.

Additionally, several incidents may occur within the same insurance interval, i.e., within an annual insurance agreement with an annual premium. The aggregated expected utility of several incidents would, therefore, be higher than what is computed for this thesis.

Concluding that while the current values return negative expected utility, there may be implicit conditions that could imply that an entity will achieve positive expected utility.

7.3 Summary of Discussion

For higher probabilities, i.e., probabilities equal to or higher than 5%, the expected utility is positive for approximately all values expect at an incident length of 4 hours. Furthermore, the highest expected utility is at 0 hours of waiting period. However, this is dependent on the assumption that entities obtain optimal coverage, which we find is not often the case.

At lower probabilities (1%), the results are more heterogeneous. When given identical circumstances, the waiting period which returns the highest expected utility, will increase per hazard class. We find that for identical lengths and revenue, an entity classified as hazard class 1 will achieve the highest expected utility at a shorter waiting period, compared to an entity classified as hazard class 5.

For lower revenues, based on the paradigm from utility theory, an entity will rank choice based on "choiceworthiness". An entity will thus not prefer to insure since there is negative expected utility related to lower revenues, i.e., $50 000 000 and $100 000 000, when exposed to lower probabilities. This will shift to positive either with increasing revenue, implying that larger entities have a higher return on insuring, or for higher probabilities of incidents indicating that there is higher return

insuring when exposed to more probable risk. When the probability is increasing, the optimal waiting period will decrease, converging towards a 0-hour waiting period.

This suggests that the shortest possible waiting period will generate the highest return for higher probabilities. For lower impact probabilities, the length of the optimal waiting period will increase. The optimal waiting period can be up to 10 hours, which is higher than the industry standard (8 hours). This length (10 hours) could be too long considering the nature of cyber incidents. Shorter duration of incident lengths, i.e., 4-, 8-, and 12 hours, returns negative expected utility for most parameters when there are low probabilities of impact, which may implicate an immature cyber insurance product.

An uncertainty is that some implicit entity factors may not be taken into account, which then in turn may influence the choice of insuring and at which waiting period. However, the results are based on the utility theorem, and the following calculations performed, whereas further research may be inclined to include complex circumstances such as these implicit factors.

For shorter incident lengths, entities should insure for cyber-related business interruption at a waiting period often shorter than what is standard (8 hours). However, the insurance product is still premature, and there is an urgent need for further research, investigation, and development of adequate tools to aid in the development of sustainable cyber-insurance products.

8 Final Conclusion

This thesis assesses which level of time retention achieves the highest expected utility for an entity, while insuring against business interruption caused by a cyber incident, using cyber insurance. Further questioning whether the current conditions for cyber-related business interruption coverage is adapted to the current cyber risk faced by companies.

We analyzed the premium calculation in the cyber insurance policies of seven major insurance carriers, where all seven policies were publicly available and a part of the admitted market. To ensure that the data was representative of the industry, two policies were omitted from the analysis. The remaining five policies were used to

calculate the average premium of the industry for cyber related business interruption coverage, relative to retention levels at 0-12-, 24-, and 48 hours. The calculated premium was used to develop a model based on expected utility theory. The model estimates the expected utility of different time retentions under cyber insurance, at revenue levels in millions of $50-, $100-, $250-, $500-, and $1 000.

Our findings are, that for higher levels of incident probabilities, i.e., 5% and 10%, there is a positive expected utility for all revenues at incident lengths of 12-, 18-, and 24 hours. While there is a negative expected utility for incident lengths of 4- and 8 hours, at some levels of revenue and hazard classes. Furthermore, for the values returning positive expected utility, all values will return the highest expected utility at a 0-hour waiting period. Justified by the utility theorem, entities exposed to probabilities higher or equal to 5% should insure and choose the lowest waiting period possible. However, insurance carriers are found to refrain from offering short waiting periods.

At lower levels of probabilities, i.e., 1%, revenues of $50 000 000 and $100 000 000 returned negative expected utility at all incident lengths and hazard classes. This leads to the conclusion that entities in this revenue range should not insure for cyber-related business interruption. For increasing revenues from $250 000 000 and up to $1 000 000 000 there were positive expected utility at incidents lengths of 12-24 hours. Additionally, higher hazard classes and/or revenue increased the waiting period, which returned the highest expected utility, advocating the notion that there is not a standardized length of waiting period, which returns the optimal expected utility for all entities.

Furthermore, there were no waiting periods above 10 hours which were found to return the highest expected utility, and for most values, the optimal waiting period converges towards 2 hours. At incident lengths equal to or lower than 8 hours, there were no values that returned positive expected utility, indicating that business interruption coverage for lower probabilities of incident does not fit the short incident lengths of cyber risk and its fast-changing nature. An entity given a choice based on expected utility will, therefore, not insure when exposed to these parameters.

Conclusively, the models' findings demonstrate that the current cyber-related business interruption- and time retention levels in cyber insurance are not well adjusted and adapted to entities' present cyber risk exposure, particularly entities classified as SMEs.

The findings of this thesis and the current lack of data on cyber incidents and its consequences, suggest that there is a need for future research to be carried out. There exists an sufficient amount of research on the nature of cyber incidents and cyber insurance. However, there is, in our view, a need for more in-depth research on the elements of cyber insurance, especially on how its individual and composed elements affect the risk mitigation of the insured. Further research on other methods of retention for cyber-related business interruption coverage, such as self-insured retention and franchise deductible, can also be suggested.

9 References

9.1 References in General

Accenture Security & Ponemon Institute. (2019). The cost of cybercrime. Ninth annual cost of cybercrime study: Unlocking the value of improved cybersecurity protection. Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

A.P. Møller – Mærsk A/S. (2017). Annual report 2017. Retrieved from https://investor.maersk.com/static-files/250c3398-7850-4c00-8afe-4dbd874e2a85

Autor, D., MIT & NBER. (2016). Lecture Note 17: The Market for Risk. In 14.03/14.003, Microeconomic Theory and Public Policy, Fall 2016. Retrieved from https://ocw.mit.edu/courses/economics/14-03-microeconomic-theory-and-public-policy-fall-2016/lecture-notes/MIT14_03F16_lec17.pdf

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis. Geneva Papers on Risk and Insurance, 40 (1). http://dx.doi.org/10.2139/ssrn.2577286

Böhme, R. & Kataria, G. (2006). Models and Measures for Correlation in Cyber-Insurance. Workshop on the Economics of Information Security. Retrieved from https://www.econinfosec.org/archive/weis2006/docs/16.pdf

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101. https://dx.doi.org/10.1191/1478088706qp063oa

Braun, V. & Clarke, V. (2013). Successful qualitative research: A Practical Guide for Beginners. Retrieved from https://www.researchgate.net/publication/256089360_Successful_Qualitative_Research_A_Practical_Guide_for_Beginners

Briggs, R. (2014). Normative theories of rational choice: Expected utility. Stanford Encyclopedia of Philosophy. Retrieved from: https://plato.stanford.edu/entries/rationality-normative-utility/

Burnecki, K., Nowicka-Zagrajek, J., & Wyłomańska, A. (2005). Pure risk premiums under deductibles. Statistical Tools for Finance and Insurance, 427-452. https://doi.org/10.1007/3-540-27395-6_19

Cambridge Dictionary. (n.d). Business Interruption. Cambridge Dictionary. Retrieved from https://dictionary.cambridge.org/dictionary/english/business-interruption

Cebula, J., J. & Young, L., R. (2010). A Taxonomy of Operational Cyber Security Risks Version 2. http://dx.doi.org/10.13140/RG.2.2.23973.91363

CIAB. (n.d.). The Role of Insurance Intermediaries. Retrieved 17. June 2020 from https://www.ciab.com/wp-content/uploads/2017/04/RoleOfInsInt.pdf?fbclid=IwAR1tDld8lQHsqLYs68-yMZrw5eoWVP6MKKC8aJQHgUqMy8LBPVV6ECZ-tck

Cisco. (n.d.). What Are the Most Common Cyber Attacks?. Retrieved 25. May 2020 from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~how-cyber-attacks-work

CISA. (2019). Assessment of the Cyber Insurance Market. Department of Homeland Security: Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov/sites/default/files/publications/19_1115_cisa_OCE-Cyber-Insurance-Market-Assessment.pdf

CSIS & McAfee (2018). The Economic Impact of Cybercrime - No Slowing Down. Executive summary on report by McAfee and CSIS, 1-4, Retrieved from: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

Cohen, G. (n.d). Downtime, Outages and Failures - Understanding Their True Costs [Blog Post]. Retrieved April 29. 2020, from https://www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html

Deloitte. (December, 2016). Business Interruption insurance claims – contentious areas. Retrieved from https://www2.deloitte.com/nz/en/pages/forensic-focus/articles/business-interruption-insurance-claims-contentious-areas.html

Emrich, C. T. & Czajkowski, J. (2013). Reinsurance. In K. B. Penuel., M. Statler & R. Hagen (Eds.). *Encyclopedia of crisis management*, 1, 805-806. https://doi.org/10.4135/9781452275956.n277

Eling, M. & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance?, Journal of Risk Finance, 17(5), 474-491. https://doi.org/10.1108/JRF-09-2016-0122

ENISA., Robinson, N., & Rand Europe. (2012). Incentives and barriers of the cyber insurance market in Europe. Retrieved from https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe

ESI Thoughtlab. (2019). The Cybersecurity Imperative Pulse Report. Retrieved from: https://www.a51.nl/sites/default/files/pdf/the-cybersecurity-imperative-pulse-report.pdf

ESI Thoughtlab. (2020). About Us. Retrieved from: https://econsultsolutions.com/esi-thoughtlab/about/

Franke, U. (2017). The Cyber Insurance Market in Sweden. Computers & Security, 68, 130-144. https://doi.org/10.1016/j.cose.2017.04.010

Frumento, E. & Dambra C. (2019). The role of intangible assets in the modern cyber threat landscape: the HERMENEUT Project. European Cyber Security

Journal, 5(1), page 56. Retrieved from https://www.researchgate.net/publication/330900994_The_role_of_intangible_assets_in_the_modern_cyber_threat_landscape_the_HERMENEUT_Project

Gerking, T. C., & Smith, D. B. (2017). Insurance when the internet goes down. Risk Management, 64(1), 16-17. Retrieved from https://search-proquest-com.ezproxy.library.bi.no/docview/1870564452?rfr_id=info%3Axri%2Fsid%3Aprimo

Greenberg, A. (August 22, 2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenwald, J. (October 24, 2016). Specialty market keeps grip on cyber risk. Retrieved from https://www.businessinsurance.com/article/00010101/NEWS06/912310137/Specialty-market-keeps-grip-on-cyber-risk

Gupta, P. K. (2008). Fundamentals of insurance (2nd ed.). Mumbai, India: Himalaya Publishing House.

Harding, T., S. & Whitehead D. (2013). Analysing data in qualitative research. In Z. Schneider & Dean Whitehead (Ed.), Nursing & Midwifery Research: Methods and Appraisal for Evidence-based Practice (4th, p.141-160). Elsevier-Mosby.

Hiscox. (2019). Cyber Readiness Report 2019. Retrieved from https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

Hydro. (2019). Annual report 2019. Retrieved from https://www.hydro.com/Document/Index?name=Annual%20report%202019%20web.pdf&id=506433

Insurance Information Institute. (n.d.). Understanding your insurance deductibles Know how your deductibles work to prevent surprise costs—and save money. Retrieved 5. April 2020 from: https://www.iii.org/article/understanding-your-insurance-deductibles

Insureon. (June 25, 2018). Admitted vs. non-admitted insurers: a guide for insurance agents. Retrieved from https://insureonsolutions.com/news/admitted-vs-non-admitted-insurers-a-guide-for-insurance-agents

IRMI (International Risk Mangement Institute). (n.d.a). Hazard Class Pricing. Retrieved 20. May 2020 from: https://www.irmi.com/term/insurance-definitions/hazard-class-pricing

IRMI (International Risk Mangement Institute). (n.d.b) Underwriting Guidelines. Retrieved 23. June 2020 from: https://www.irmi.com/term/insurance-definitions/underwriting-guidelines

Kaas, R., Goovaerts, M., Dhaene, J., & Denuit, M. (2008). Utility theory and insurance. In Modern actuarial risk theory: Using R. https://doi.org/10.1007/978-3-540-70998-5_1

Kesan, J. P., Majuca, R. P., & Yurcik, W. J. (2004). The Economic Case for Cyberinsurance. University of Illinois College of Law: Law and Economics Working Papers. Retrieved from: https://law.bepress.com/uiuclwps/art2/

Kesan, J., Majuca, R. and Yurcik, W.J. (2006), "Cyber-insurance as a market-based solution to the problem of cyber security – a case study", WEIS, 1-46 Retrieved from https://www.semanticscholar.org/paper/Cyber-insurance-As-A-Market-Based-Solution-To-The-Kesan-Majuca/fbacfbf013bae9077165280e1da04438d0b0c1d8

Kuru, D. & Bayraktar, S. (2017). The effect of cyber-risk insurance to social welfare. Journal of Financial Crime, 24(2) 329-346 Retrieved from: https://doi.org/10.1108/JFC-05-2016-0035

Laeven, R., J., A. & Goovaerts M. (2008) Premium Calculation and Insurance Pricing. Encyclopedia of Quantitative Risk Analysis and Assessment. https://doi.org/10.1002/9780470061596.risk0364

Małecka, M. (2019). The normative decision theory in economics: a philosophy of science perspective. The case of the expected utility theory. Journal of Economic Methodology, 27(1), 36-50. https://doi.org/10.1080/1350178X.2019.1640891

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. Computer Science Review, 24, 35-61. https://doi.org/10.1016/j.cosrev.2017.01.001

Marsh. (2012). Marsh Insights Property - Fall 2012. Retrieved from https://www.marsh.com/pr/en/insights/research/business-insurance.html

NAIC. (n.d.) About. Retrieved from https://content.naic.org/index_about.htm

National Cyber Security Alliance. (2019). New Survey Shows Majority of Small Businesses Believe They are a Likely Target for CyberCrimes; More Than a Quarter have Experienced Data Breach in Last Year. Retrieved from https://nationalcybersecurity.com/nationalcybersecuritymonth-new-survey-shows-majority-of-small-businesses-believe-they-are-a-likely-target-for-cybercrimes-more-than-a-quarter-have-experienced-data-breach-in-last-year/

NAIC (National Association of Insurance Commissioners). (2019). NAIC Releases 3rd Annual Report on Cybersecurity Insurance and Identity Theft Coverage Supplement. Retrieved from https://content.naic.org/article/news_release_naic_releases_3rd_annual_report_cybersecurity_insurance_and_identity_theft_coverage_supplement.htm

Neumann, J., v. & Morgenstern, O. (1944). The Theory of Games and Economic Behavior. Princeton University Press. Retrieved from https://www-dawsonera-com.ezproxy.library.bi.no/readonline/9781400829460

OECD. (2017). Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, p.93-109. http://dx.doi.org/10.1787/9789264282148-en

OECD. (2018). The Institutional Structure of Insurance Regulation and Supervision. Retrieved from https://www.oecd.org/finance/The-Institutional-Structure-of-Insurance-Regulation-and-Supervision.pdf

Öğüt, H. Raghunathan, S. & Menon, N. (2011). Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and Observability of Self-Protection. Risk Analysis, 31(3), 497-512. https://doi.org/10.1111/j.1539-6924.2010.01478.x

PartnerRe & Advisen. (2019). Cyber Insurance – The Market's View. Retrieved from https://partnerre.com/wp-content/uploads/2019/10/Cyber_Insurance_The_Markets_View_2019-1.pdf

Perlroth, N., Scott, M., & Frenkel, S. (2017, 27. June) Cyberattack Hits Ukraine Then Spreads Internationally. The New York Times. Retrieved from https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Pohl, S. & Iranya, J. (2018). *The ABC of Reinsurance*. Karlsruhe: Verlag Versicherungswirtschaft.

Ponemon Institute & Radware. (2012). Cyber Security on the Offense: A study of IT Security Experts. Retrieved from https://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf

Raviv, A. (1979). The Design of an Optimal Insurance policy. American Economic Review, 69(1) 84-96. Retrieved from www.jstor.org/stable/1802499

Research Methodology. (n.d.) Purposive sampling. Retrieved from https://research-methodology.net/sampling-in-primary-data-collection/purposive-sampling/

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk?. Journal of Cybersecurity, 5(1), tyz002. https://doi.org/10.1093/cybsec/tyz002

"Salty" Schumann, ,C.P. (2013). BUSINESS INTERRUPTION LOSSES. Valuation Strategies, 16(6), 26-33. Retrieved from https://ezproxy.library.bi.no/login?url=https://search-proquest-com.ezproxy.library.bi.no/docview/1425514473?accountid=142923

SERFF. (n.d.). About the system for electronic rates & forms filing (SERFF). Retrieved from https://www.serff.com/

Shackelford, S., J. (2012). Should your firm invest in cyber risk insurance?. Business Horizons, 55(4), 349-356 https://doi.org/10.1016/j.bushor.2012.02.004

Szpiro, G. (1985). Optimal Insurance Coverage. The Journal of Risk and Insurance, 52(4), 704-710. http://dx.doi.org/10.2307/252315

Toregas, C., & Zahn, N. (2014). Insurance for Cyber Attacks: The Issue of Setting Premiums in Context. Cyber Security Policy and Research Institute, The George Washington University. Retrieved from https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/cyberinsurance_paper_pdf_0.pdf

Trefis Team. (Sep 11, 2019). How Could The Recent Data Breach Affect Capital One's Stock?. Forbes. Retrieved from https://www.forbes.com/sites/greatspeculations/2019/09/11/how-could-the-recent-data-breach-affect-capital-ones-stock/#473f6e3237b7

University of Minnesota Libraries Publishing. (2011). 7.1 The Concept of Utility. Retrieved from https://open.lib.umn.edu/principleseconomics/chapter/7-1-the-concept-of-utility/

Vistage, Cisco & NCMM. (2018) Cyberthreats and solutions for small and midsize businesses. Retrieved from https://www.vistage.com/wp-content/uploads/2018/04/Cybersecurity-Research-Note.pdf

Wolferen, J., v. Inbar, Y. & Zeelenberg, M. (2013). Moral hazard in the insurance industry. *Netspar Panel Paper*, 33, 1-76. Retrieved from https://www.researchgate.net/publication/235988864_Moral_hazard_in_the_insurance_industry

Zhang, J. (2014). The Role of Insurance Brokers at the Formation Stage of Marine Insurance Contracts in China.*Tulane Maritime Law Journal*, *39*, 707. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/tulmar39&div=29&g_sent=1&casa_token=&collection=journals

9.2 References of Policies Accessed from SERFF:

ACE American Insurance Company (Chubb). (2019). Cyber, Digitech and PRO ERM. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131948126

Everest National Insurance Company. (2019). EVEREST CYBER ELEVATION PROGRAM. *SERFF Filing Access Pennsylvania*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131385235

Key Risk Insurance Company (Berkley). (2018). Berkley Cyber Risk Insurance - New Program Filing. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131433514

Hartford Fire Insurance Company & Twin City Fire Insurance Company (2020). CYBER PRODUCTS. *SERFF Filing Access California*. Retrieved from

https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=132400418

Philadelphia Indemnity Insurance Company. (2019). Cyber Security. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131804819

QBE Insurance Corporation. (2019). The Solution for Cyber Risk. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131915871

State National Insurance Company, Inc. (2019). CFC - Cyber Private Enterprise Program. *SERFF Filing Access Pennsylvania*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=132219798

Travelers Casualty and Surety Company of America. (2020). CyberRisk Rate and Rule Filing 2020-01-0106. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=132247837

ACE American Insurance Company (Chubb). (2019). Cyber, Digitech and PRO ERM. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131948126

Everest National Insurance Company. (2019). EVEREST CYBER ELEVATION PROGRAM. *SERFF Filing Access Pennsylvania*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131385235

Hartford Fire Insurance Company & Twin City Fire Insurance Company (2020). CYBER PRODUCTS. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=132400418

Philadelphia Indemnity Insurance Company. (2019). Cyber Security. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131804819

QBE Insurance Corporation. (2019). The Solution for Cyber Risk. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131915871

State National Insurance Company, Inc. (2019). CFC - Cyber Private Enterprise Program. *SERFF Filing Access Pennsylvania*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=132219798

Travelers Casualty and Surety Company of America. (2020). CyberRisk Rate and Rule Filing 2020-01-0106. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=132247837

QBE Insurance Corporation. (2019). The Solution for Cyber Risk. *SERFF Filing Access California*. Retrieved from https://filingaccess.serff.com/sfa/search/filingSummary.xhtml?filingId=131915871

10 Appendices

10.1 Transcription and Analysis of Interviews

Appendix A1 - Transcription and Analysis of Interview with Eirik Lund 13.01.20

Semantic Codes	Latent Codes	Transcription of Interview
Coverage of CF		Kris: For vi pratet jo om Hydro, er jo nyere det er jo det, tilgangen til polisene og tilgangen til informasjon er kanskje vanskelig sånt sett da. Mer sensitivt. Eirik: Ja det er akkurat det, det var en sånn PR fyr som var å snakket i Gjensidige om hvordan de håndterte den situasjonen og jeg stilte jo selvfølgelig spørsmål om hva som var dekket og, men han svarte bare det som står i avisen, altså de har en robust cyberforsikring (cf). De vil ikke si hvilke poster som er dekket og ikke dekket, og hvilke poster de har. Og hvilke summer de har da. Men jeg kan jo kanskje begynne med å si litt om Cyber forsikring generelt da, bar for å få inngangen til hva som vil være dekket. For det vil jo også svare på hva som sannsynligvis Maersk har dekket og ikke. Så Cyberforsikring er jo nokså nytt forsikringsprodukt og det stammer fra USA, tror jeg det er der det er det største markedet. Mats: Ja det er det vi har lest også. Eirik: Ja ikke sant, da har dere sikkert lest en god del om det. Mats: Ja Eirik: Da skal jeg ikke begynne så tidlig, men sånn de klassiske punktene på cf er jo hvis jeg kan snakke litt om Gjensidiges etterpå og markedet. Men de klassiske er jo at det dekker driftstap, og rekonstruksjons utgiftene. Det er liksom de to kjernene i cf. Ikke sant, driftstap altså at

Coverage of CF		du får nedetid. Hydro fikk jo nedetid, de fikk ikke levert som de skulle, eller som et banalt eksempel, hvis et IT selskap som lever IT tjenester også blir de hacket også er de nede, og da får de et driftstap. Og da dekker dette drifts tapet. Rekonstruksjon dekningen er jo da utgiften man trenger for å rekonstruere all dataene dine. Igjen Maersk er jo litt spesielt fordi det er så stort. Men hvis man tar et banalt eksempel; en snekker på hjørnet eller et eller annet som får datainnbrudd, og dataene er slette, så får man dekket de utgiftene for å rekonstruere dataene, ved hjelp av backup og få datasystemene opp å gå igjen. De to er kjernen i en cf. som går igjen i for både små kunde markedet (smb -markedet) som er små-, mellomstore bedrifter. Og stor kunder, så det er nok kjernen, også er det standarden i markedet er at cf har en sånn ID-tyveri dekning. og sånn varsling tjeneste, som er særlig viktig for store bedrifter, som for Maersk blir det jo veldig omfattende, men for en vanlig stor bedrift med en del kunder, må man jo etter datatilsynet og er det personvernlovgivningen, så man jo varsle om at det skjedd et datainnbrudd, hvis det er sensitiv informasjon om kunder for eksempel.
	Influence of regulations	Mats: Innen en hvis tid er det ikke det?
	Influence of regulations	Eirik: Jo kanskje kort. Du må varsle datatilsynet og kundene innen 48 timer, eller noe sånt noe.
	Influence of regulations	Kris: Ja jeg mener å ha lest det.
	Lack of data	Eirik: Ja det er ganske raskt man må være på ballen. det kan jo for store kunder være ganske kostnadskrevende og tidkrevende og få varslet på korrekt måte overfor datatilsynet og kunden. så varslingstjenesten er en viktig bit (av cf). så som det store egentlig spørsmålet til Maersk og Hydro er jo hvilke summer de har, altså hvor høye forsikringssummer har de? Fordi det som er litt spesielt med cf enn så lenge, er jo at hvis du skal tegne forsikring på et hus eller vanlig driftstap forsikring, så får du jo veldig høye summer, altså du kan forsikre den sannsynligvis til så høyt du nesten bare vil. Men med cf hvor det er så mye usikkerhet i markedet på hva er riktig prising, og det er veldig stor skade drevet, som Maersk og Hydro. Når det først smeller hos de så smeller det så innmari, så derfor koster det veldig mye å ha veldig høye summer (Forsikret). På smb markedet, de små og

		mellomstore, så er standarden i markedet på sånn 5-10 millioner totalt for alle disse dekningene. Også kan du kjøpe mer, jo høyere opp du skal, jo mer må reassuranse kontaktes og det blir en helt annen prosess, så veldig ofte for Maersk, nå vet jeg ikke helt hva Maersk hadde i dekning, men de har jo hatt enorme tap, men hvor mye de har i dekning vet jeg. Men jeg vil jo tro at de går igjennom dette reassuranse programmet sitt etter dette her skjedde, men hvor mye dekning, altså hvor mye høye forsikringssummer de får, og til hvilken pris det er vanskelig og vite. Men da er alle de store spillerne i spill, for det koster mye. Så for Maersk sin del vil jeg tro at de ikke har hatt dekning for alt. Mats: Nei, for det er vel mange som har undervurdert skadepotensialet, på grunn av mangler på eksempler for eksempel.
SMBs lagging behind		Eirik: Ja mangler på eksempler, ja og da er spørsmålet for de små- og mellomstore så er det veldig få som har cf i dag. for de store kunde markedene som er mer på ballen og vurderer sin risiko, så er det jo fler som har cf, men også der så er den en del som ikke er gode nok i forhold til dette (cybersikkerhet) enda da. Mats: Så markedet er primært store selskaper? Eirik: Ja det er de som trenger det sannsynligvis mest. I hvert fall fra et økonomisk ståsted, mens de små- og mellomstore, hvis de ikke er veldig sårbare for IT, for eksempel et IT-selskap som er bare data, de ser jo at er datasystemene dems nede, så er de i skikkelig trøbbel, de får ikke levert det de skal, og de trenger kanskje hjelp til å få dette opp å gå igjen.
SMBs lagging behind		Kris: Selvfølgelig. Jeg lurte bare på sånn reinsurance, må den som skal forsikres kontakte disse, eller er det forsikringsselskapet også kontakter de re insurance markedet? Eirik: Det kan jeg ikke svare på for alle, men hos oss (Gjensidige) og som jeg vil tro er veldig standard, er at det er en som er såkalt "lead", det er de som selger forsikringen, som for eksempel gjensidige, så er det gjensidige som selger cf, så er det hvis det kommer over visse forsikringssummer, altså at de skal ha veldig høye

	Demands put on customers	summer/nokså høye summer, eller det er en veldig stor kunde, altså høy omsetning, så tar man kontakt med reassurandøren sin. også har man noen retningslinjer, hvor man må stille ganske mange spørsmål til kunden, om hvordan de håndterer cyber risikoen sin i dag. fra alt til IT systemer og om de har en slags beredskapsplan hvis det skulle skje noe. da kommer det sannsynligvis en del krav til disse kundene, som Maersk og Hydro, hvertfall nå etter dette har skjedd (de to cyber angrepene), og sånne store kunder de får en del ganske innfløkte spørsmål om hvordan de er forberedt på en sånn hendelse. for da ønsker man jo selvfølgelig å minimalisere tapet, og er man godt forberedt, så får man datasystemene kanskje raskere opp å gå hvis man har ordentlig backup. og selvfølgelig anti-virus program, veldig sånt banalt at du prøver å minimere risikoen for at det skjer. Mats: Men de kravene blir lagt på etter hvert eller?
	Demands put on customers Emerging market	Eirik: Ja, de kan nok bli lagt på etter hvert. Som for eksempel Hydro, hvis de skal fornye (cf) så vil det nok bli stilt nye krav, hvis ikke de hadde disse kravene allerede. Jeg tror det er svaret på det altså. I smb markedet er det sånn, i hvertfall i Norge og i Norden så er det jo Gjensidige, IF og Kodan og alle disse her som er de store, og der er det smb-markedet som er det store segmentet. Og der er det ganske få krav til sikkerhet, det er fordi man ønsker å få solgt; man ønsker å pushe ut cyber forsikring. Så da er det bare krav til at man har backup og at man har et antivirusprogram, og thats it. På nokså lave summer, skal man opp på høyere summer er det flere krav som blir stilt til kunden. På Maersk caset, er det forsikringssummer som er det store spørsmålet, men vi vet jo at de sannsynligvis hadde et stort tap, nå har ikke jeg vært inne i årsrapporten deres, men Hydro sa jo selv at de hadde en robust cyber forsikring. Og i den siste kvartalsrapporten deres, så la de frem at de hadde fått utbetalt noe på forsikringen, og at de også forventet å få ytterligere utbetalinger. Men de kunne ikke regnskapsfører dette enda, grunnet enkelte regnskapsprinsipper, som sier at man ikke kan bokføre det, før det er helt sikkert.

Coverage of CF	Emerging market Professional support	Kris: Jeg vet ikke om jeg husker, men jeg mener å ha lest at det kun var 6-7% som ble dekket av tapet, gjennom cf, alene da men. Eirik: Hydro eller Maersk? Kris: Hydro. Maersk hadde jo ikke noe, de forsøkte å ta det inn i de vanlige polisene sine, men de hadde ikke noe spesifikk cf. De sa det i årsrapporten sin etterpå at nå har de skaffet seg en cf. Eirik: Så bra da er dere mer oppdatert enn meg her. Kris: Ja, vi har på en måte lest oss opp litt sånt sett da. Også litt om informasjon, om vi får tilgang til forsikringspoliser, eller hvor konfidensielt det egentlig er da? Eirik: Det er jo ganske standardisert der. jeg må ta en liten sjekk med arbeidsgiveren min da om det er greit, men dere skal hvertfall kunne få høydepunktene, jeg tror dere skal kunne få polisene, men det skal jeg sjekke. jeg skal hvertfall sjekke hva dere kan få da. Fordi gjensidige cf er jo en standard i markedet, det er under utvikling, men de er veldig like enn så lenge, triggeren er at det skjer et datainnbrudd, at noe eller noen må ha kommet seg inn i datasystemene, også så lenge det har skjedd, så kommer den beredskapen i gang, da kan man ringe hvertfall til gjensidige. Alle disse forsikringsselskapene har for det meste alliert seg med et IT sikkerhetsselskap, som da foretar undersøkelser om det er skjedd et datainnbrudd og omfanget av det. også når det er kartlagt, så får man den hjelpen man trenger, ved å få rekonstruert data og får dekket driftstap osv. Og disse varslings tjenestene. Mats: Men, tap med tanke på omdømme, og immaterielle verdier og sånn? Eirik: Ja, det er noen som dekker det, det er stor-kunde segmentet igjen. Det kan også være dekket på cf. Mats: Ja, for vi har lest noe om det, og da er ofte problemet som går igjen verdisettingen av det immaterielle tapet. Eirik: Akkurat, for hva er det ikke sant. Det en del har er PR rådgivning, hvis du er en stor nok kunde så er dette

		negativ pr, og da gjelder det å ha en PR strategi, og dette kan man også få dekket på en cf, men det er jo igjen stor-kunde markedet typisk. For da kan du ha bruk for hvordan du skal håndtere dette her. Kris: Da blir polisen skreddersydd til stor kunden? Eirik: Ja. Kris: For å passe deres behov? Eirik: Ja. Det kan nok være noen som tilbyr det til de små (selskapene) også, men på en måte snekkeren på hjørnet har ikke behov for PR rådgivning. Så det er til de mellomstore og store kundene. Kris: Hvordan verdsetter dere premiumene på dette?
	Pricing and risk asseseme nt	Eirik: Det kommer an på hvilke dekninger du skal ha og summer, men så skiller de jo også på type selskap. Så prisingen er forskjellig ut i fra om du blir vurdert som høy risiko eller lav risiko, og det kommer jo an på om du for eksempel leverer fysiske tjenester så er jo sannsynligheten for nedetid eller driftstap mindre, enn hvis du leverer kun for eksempel en IT tjeneste; et IT selskap. Som evry for eksempel. Er evry nede taper du penger hver dag, da stopper det helt opp, men driver du en form for fysiske tjeneste skal det kanskje mer til. Du kan sannsynligvis fortsette og levere tjenestene dine, selv om dataen er nede, i hvertfall for en periode, kanskje. Men Hydro levere jo fysiske tjenester så de fikk jo nedetid de også. Men det er en vurdering, mellom hva slags type selskap, hvilke dekninger du skal ha og hvor høye forsikringssummer du skal ha. Og hvor stor bedriften skal ha, altså i omsetning. Mats: Men på de mindre (selskapene), er det et fast prosent beløp? Eirik: Jeg kan si Gjensidiges minstepris da, og det er veldig lavt, er rundt 1500 kr. for de absolutt minste selskapene med lave forsikringssummer, og det går igjen blant aktørene i Norge, de rimeligste ligger på rundt 2000-2500 kanskje. Jeg mener IF har kanskje satt ned sin, hvis dere går inn på gjensidige.no, kan dere gå inn å søke på organisasjonsnummer (til bedrifter), så kan dere få tilbud på pris. Det er en slags nettkalkulator hvor man kan

		teste. I hvert fall gjensidige har det, og IF hadde det, men jeg tror de har tatt den ned. Og Trygg og Kodan kanskje, hvis dere går inn der, får dere kanskje en feeling på hva det koster. Kris [00:13:23]: Dere kjenner egentlig til forsikrings prisene til de andre aktørene i markedet, det er vel standardiserte kontrakter? Eirik [00:13:31]: Ganske standard, hvertfall for små- og mellomstore, også for de store kan det være litt ulikt, for det kan være litt skreddersydd, etter behov. Men der også er det nokså likt. Mats: [00:13:42]: Når et stort selskap kommer i markedet og skal hente inn (tilbud) da går han vil til både gjensidige og IF og de andre? Eirik [00:13:50]: Ja en stor kunde vil jo gå til sannsynligvis mange, men noen av de har kanskje program hos AEG, hvis de har større program, de vel mest sannsynligvis begynne der de har forsikringspolisene sine i dag. De aller fleste har dette samlet ett sted, også er det noen som shopper litt og har litt forskjellig på ulike steder. Kanskje fordi de vil holde forsikringsselskapene litt på ballen og gi dem gode priser. Men et forsikringsselskap vil jo også si at hvis man samler alt oss hos, så får du en bedre pris. Men det er en annen historie. Men jeg ville sannsynligvis begynt der de har polisene/forsikringen(e) i dag. Så kan det jo hende det er noen kunder som ønsker veldig store summer, så kan du tenke at et forsikringsselskap ikke kan tilby det de ønsker, de vil jo sannsynligvis prøve og løse det, da for eksempel ved å se om de kan få noe inn på et reassuranseprogram eller lignende, men hvis ikke så må man henvise deg til et større forsikringsselskap. Kris [00:14:52]: Maersk hentet jo inn JLT og Miller. Men Maersk er jo så store, så de er sikker nødt til det. Er jo så store eiendeler, både fysiske og ... (immaterielle). Eirik [00:15:03]: Ja det er akkurat det, så de har sikkert (forsikring) litt forskjellige steder. Og har et helt annet program.
	Customers sensitivity to price	

		Mats [00:15:07]: Men da går det også over landegrenser, det er ikke noe begrensninger i om det skjer i Latvia, hvis de har et kontor der eller om det skjer i Oslo? Eirik [00:15:15]: Ja, altså du tenker på? Mats [00:15:20]: Om det går globalt? Eirik [00:15:21]: Ja, hvis du er et globalt selskap, så trenger du forsikring lokalt, så det er sikkert derfor hvis du har fabrikker rundt omkring, så trenger du kanskje en global forsikrings aktør, som kan levere deg det du trenger. Slik at du kan få hjelp hvis (f.eks.) Hydro blir hacket ett eller annet sted i USA, så er det kanskje lettere for dem å ha noen der lokalt, enn at gjensidige skal komme der og gjøre undersøkelser, så det er nok et vesentlig poeng. Så de (Hydro) vil jo søke en global forsikringsaktør. Kris [00:15:58]: Er det en database i Norge for forsikringspoliser? For vi leste om at i USA, så har du SERFF, der hvor alle må legge inn etc. Og jeg lurte på om det er en database som vi kunne fått tilgang til, der hvor alle Norske forsikrings aktører må sende inn og få godkjent av staten om dette er lovlig. Eirik [00:16:18]: Nei, det er ikke noe sånt system, for sånn 20-30 år siden, så drev forsikringsselskapene og ringte til hverandre for å få polisene til hverandre, slik at de kunne se hva de dekket og tok i pris. Men det var ikke populært fra et konkurranse ståsted. Så man deler ikke på den måten i dag. Men det kommer krav fra EU om standardiserte produktark, hvor det skal stå beskrevet ganske godt hva som er dekket og ikke, men detaljene i polisene de er ikke offentlig tilgjengelig, da må man innhente tilbud. Men man får jo tilbud fra alle; en sånn 5-6 selskaper, så det er ikke så hemmelig, de er veldig like. Så det kanskje mest interessante hvis jeg skulle sett på konkurrenter, er jo å se hva som dekkes, men også se ca hva dette koster hvilket nivå ligger de på? Kris [00:17:21]: Ja selvfølgelig, sammenligne prisnivået. Eirik [00:17:22]: Ja så det er ikke noe særlig database, men man kan jo alltids ringe og høre, hvis dere ringer IF og AEG, og sier at dere skriver oppgave og hører om dere
	Influence of regulations	

		kan få en polise. Jeg tror det er store muligheter for å få noen poliser. Kris [00:17:40]: Ja de er kanskje fleksible sånn sett, når man ser hvordan du (Eirik) takler det, så er det jo mest sannsynlig fleksibilitet. Eirik [00:17:44]: Ja, for det er stort sett veldig likt ikke sant, man selger jo dette til masse kunder, så det er ikke slik at det er kjempe hemmelig, hva som står i disse polisene. Men om dere kan få en hel polise, det skal jeg sjekke. Kris [00:17:58]: Ja det hadde vært kjempe hyggelig det. Eirik [00:17:58]: Jeg kan jo kanskje ta bort noen sider, eller hva det skal være. Ja jeg skal se hva jeg får til. Kris [00:18:05]: Altså, vi har sett litt på tvetydige betydninger, jeg vet ikke om du fikk med deg den Mondelez saken (angrep)? De hadde egentlig cf, men så mente Zurich insurance group at dette falt under krigen klausulen der. Så det er rettsak nå om at de ikke får dekket. Eirik [00:18:23]: Ja riktig, den kjenner jeg til. Mats [00:18:24]: Det var jo fordi viruset var russisk støttet. Eirik [00:18:27]: Det var nettopp, for det var vel om det var krigshandling eller noe sånt noe? Jeg har lest om det, og hørt om det for en god stund siden. Men jeg har ikke hørt om det har kommet noe ut av det, eller vært noen utvikling i saken. Mats [00:18:39]: Det vi har lest/skjønt hittil er at det mange som har cyber forsikringer (avbrutt av gråtende barn) ... men som da selv ikke har skjønt hva den dekker. Fordi det er såpass nytt. Eirik [00:19:21]: Det tror jeg er riktig, det er mange aspekter, hvor man ikke helt skjønner hva som er dekket, eller ikke dekket. I forsikringsmarkedet så går jo ting veldig treigt, men i cf så går det relativt raskt, det kommer en del nye ting som dekkes. For eksempel har noe begynt å dekke datakrasj, uten at det er noe hacking eller virus.
	Emerging market	

	Lack of understanding of coverage	Mens andre ikke dekker det, da de mener at dette er noe bedriften må dekke, det er risikoen ved å drive selskap. Skadeforsikring er jo slik at de må skje en skade, så da nærmer det seg en litt an tjeneste enn skadeforsikring. Det er nok noen som tror at hvis dataen krasjer så er de dekket av cf. Og noen har det dekket og da. Det er jo et eksempel på noe som enkelte tror er dekket. Kris [00:20:30]: Har du opplevd mange av de problemstillingen; med kunder som tenker at de er dekket, men ikke er det? Eirik [00:20:35]: Ja, det er noen som har hatt datakrasj, de tenkte at det var dekket, men det var det ikke. Andre tilfeller da, jeg kommer ikke på noe annet nå på stående fot, jeg skal tenke på det. Mats [00:20:54]: Noe med blanket bonds, forsikring relatert til det ansatte kan gjøre internt, ja hva om en ansatt hacker, er det da blanket bonde eller cf som dekker? Eirik [00:21:07]: Ja, jeg kjenner jo ikke til alt som er dekket, men gjensidige dekker jo da hvis det skjer et datainnbrudd. Så hvem som har gjort det er irrelevant. Men det kan være omstendigheter som gjør at man må ta forbehold. Etter forsikringsavtaleloven så er det slik at hvis grovt uaktsomt har fremkalt forsikringstilfellet, altså hvis det er ett eller annet du gjør som gjør at det er for lett, ikke har noen mekanismer som hindrer at det skjer, så kan det tenkes at det er uaktsomt. Men utgangspunktet er at det må skje datainnbrudd. Så hvem som har gjort det skal egentlig være irrelevant. Kris [00:21:45]: hvor går egentlig det skillet mellom det som er grovt uaktsomt i internett sfæren? Eirik [00:21:50]: Utgangspunktet er at det er dekket. Men så er det grovt uaktsomhet, hvor det skal ganske mye til. Jeg har ikke et godt eksempel, men det kan være bransje anbefalinger som ikke er fulgt, for eksempel i gjensidige, som er et stort børsnotert selskap så er det mye compliance regler, mye compliance om hvordan man skal lære opp ansatte, hva man skal passe på og hva man ikke skal gjøre, passe på at ansatte ikke tilgang til alle IT systemer, hvis jeg for eksempel enkelt kunne logget meg

		inn og begynt å hacke, lett tilgang for å ødelegge, så kunne det kanskje vært spørsmål om at det kanskje ikke var hacking. Det kan være sånne ting, når jeg tenker rent teoretisk. Jeg har ikke vært borti noen tilfeller hvor det har vært brukt, men for helhetens skyld, så må jeg nevne at det kan tenkes at det blir avslått. Mats [00:22:51]: Men du sier at kravet er datainnbrudd, har dere en klar definisjon av det. Eirik [00:22:56]: Ja vi har definert det i erstatningsreglene, i cf'en så er det en definisjon på det. Så hvis dere får polisen, som jeg tror dere kan få så skal det stå der, og der står det definert hva som er et datainnbrudd. Og tanken med den definisjonen er jo at den er veldig vid, det er ikke der vi skal i gåseøyne "mislede kunden", så det er en veldig bred definisjon av et datainnbrudd. Det er da hvis noen eller noe som har kommet seg inn i datasystemet som ikke skal være der, så er det et datainnbrudd. Så det skal være lavterskel, det skal være enkelt å få dekket dette data innbrudds kravet. Kris [00:23:37]: Jeg bare tenkte på etter den Maersk-hendelsen, var det noen reaksjon i polisene, hadde dere noe møte, eller måtte endre på noe? Eirik [00:23:46]: Ikke Maersk angrepet. Kris [00:23:49]: Det var jo flere selskaper som ble truffet selvfølgelig, men akkurat den hendelsen der?
	Emerging market	Eirik [00:23:52]: Altså, i Norden så er jo cyber forsikringsmarkedet veldig umodent. Det har begynt mer nå, men det var ganske få som tok sånne store risikoer. Da går nok de (selskapene) til større aktører enn man har her i Norden. Men nå begynner det smått å bli en modning her i Norden også. Hvor fler og fler kunder kommer og banker på døren til forsikringsselskapet sitt, og spør; "hei, vi har jo ikke cf, dette er en stor risiko". Særlig (etter) Hydro hvor det blir veldig tett på. (Hvor selskapene) tenker at dette kan jo skje oss også, så etter det har jeg merket en pågang av kunder som ønsker å finne ut av hva deres cyber eksponering, hva er dekket i dag, hva er ikke dekket i dag, hva i så fall trenger man å kjøpe av ekstra dekning, hvilke summer trenger de, hva koster det. Så det er kommet inn mer spørsmål som gjør

		at disse forsikringsselskapene blir enda mer tvunget til å begynne å planlegge litt for fremtiden, om hvordan de skal håndtere disse stor kundene når de kommer. For man ønsker jo hjelpe kundene sine, også da går man tilbake til å ha gode nok reassuranseavtaler, for man ønsker ikke å ta den risikoen alene. Det er for stort alene. Mats [00:25:10]: Sånn, hvordan estimerer dere risikoen?
	Emerging market Role of reinsurance	Eirik [00:25:18]: Ja, igjen der er vi i Norden et umodent marked, så jeg vil jo påstå at de aller fleste, også de største markedene i Norden, de har jo en reassurandør i ryggen, som har mer erfaring på hva som skal dekkes og på prising, så veldig mange får nok en del guiding av disse reassurandørene Kris [00:25:34]: Så da går de til sine, kall det underleverandører, hvis gjensidige jeg vet ikke hvilke reassurandører gruppe eller hvem dere har. Da går dere til dem og spør hvordan de ville gjort det?
	Role of reinsurance Emerging market Role of reinsurance	Eirik [00:25:46]: Ja ikke sant, fordi altså generelt alle forsikringsselskaper har reassurandører på alle risikoene sine. Det er jo ikke bare cyber dette her, det er jo på bygninger og eiendommer og driftstap, så har man jo reassuranseprogram, også er det likt ulikt på hvor tidlig innslagspunkt det er, man har jo en egen risiko ikke sant, så hvis den kommer opp til en viss sum, så går det på reassuranse programmet. Og cf som er nokså nytt i Norden, i Norge var det vel IF som var først ute, vi snakker sånn 3-4 år siden. Og da starter man jo helt på scratch, også trenger man reassuranse, da går man til en reassurandør og har dialog med dem, om hva en cf inneholder. Hvordan skal man prise dette, og da har de aller aller fleste fått veiledning av dem da, for hvordan de skal prise, og hvem som er høy- og lav risiko. og hvordan pris modellene skal være i forhold til forsikring summer osv. Kris [00:26:44]: Men de reassuranse selskapene, er de egne selskaper, som kun jobber i dette markedet. Eller er det som AEG? Eirik [00:26:52]: Ja det er sånn Munich RE og flere andre sånne store, som driver med masse reassuranse, som har store reassuranseprogram, som igjen som er del av et

		svært nettverk. Hvor alle tar en del av kaken hvis det skulle smelle. Kris [00:27:07]: Okay, altså så de driver vanlige kommersiell virksomhet mot privatkunder, men så har de det store programmet, så de deler... Eirik [00:27:15]: Ja ikke sant, også alle forsikringsselskaper har reassuranseprogram. Så hvis et hus brenner ned så; nå kjenner jeg ikke akkurat innslagspunktet for alle disse reassuranse programmene. Jeg har ikke jobbet så mye med reassuranse, det er ikke det jeg kan best. Men det er et innslagspunkt der, for eksempel en næringsbygning, hvis det raser ned, og det kommer et tap på si 100 millioner, så vil sannsynligvis en del være dekket på reassuranse programmet. Så man betaler en premie for å ha et reassuranseprogram. Og da er det jo mange som tar en del av risikoen, ikke sant. Forsikringsselskapene forsikrer jo seg selv, det handler om å spre risiko overalt her. Mats [00:27:50]: Så man kan egentlig si at det gjensidige og andre er villige til å dekke gjennom sine forsikringer, er avhengig av hvor stort reassuransemarkedet er? Eirik [00:28:00]: Ja i hvert fall vil det komme an på hvor høy risiko forsikringsselskapet ønsker å ta, jeg kan jo ikke svare for alle, men det vil overraske meg veldig hvis noen av forsikringsselskapene i Norge som tilbyr cf og annen forsikring for øvrig, ikke har reassuranse, du må nesten ha reassuranse. Men igjen det kommer jo an på hvilke summer. Men hvis du selger på lave summer, så kan det jo skje en hendelse som gjør at 100 kunder blir rammet samtidig, typ datainnbrudd, noen hacker data, jeg vet da søren. Men at alle får nedetid, så kan jo det ramme mange samtidig, du må nesten ha reassuranse. Nå kjenner jeg ikke de regulatoriske reglene, men myndighetene er jo opptatt av at forsikringsselskapene skal være solide. Nå snakker jeg meg kanskje bort her, men om det er krav til reassuranse er jeg litt usikker på. Men det er jo krav til egenkapital, du skal ha en ganske høy egenkapital for å drive forsikringsselskap, det kan sikkert faren min mer om enn meg. Dere får høre med han om akkurat det. Men alle som tilbyr cf i Norge har reassuranse, noe annet ville overrasket meg veldig.
	Damage potential	

	Damage potential	Kris [00:29:18]: Har du noe mer å komme med da eller? Mats [00:29:20]: Jeg har ikke noe akkurat nå Eirik [00:29:21]: Jeg kan sjekke litt rundt akkurat på Hydro, om det har vært noen diskusjoner eller om det er et eller annet jeg kan komme med. Fordi dere har jo lest dere opp, dere vet jo hva som har skjedd og omfanget av det. Det er jo flere artikler om det, de brukte jo Deloitte eller noe sånt, det var jo flere 100 konsulenter som jobbet med dette i hvert fall et år eller noe sånt noe. Mats [00:29:49]: I sammenheng med Hydro? Eirik [00:29:51]: Nei, med Maersk mener ja. For å få dette opp å gå igjen, holde det flytende. Kris [00:30:00]: Det kostet dem 250-300 millioner dollar. Er noen sinnsyke penge mengder, bare på et angrep, og dette var jo ikke de som ble truffet mest. Mondelez ble jo truffet for 100 millioner dollar. Også merk et legemiddelselskap, 900 millioner dollar kostet det. Eirik [00:30:17]: Ikke sant, så de tapspostene til Maersk, den ene er jo driftstapet, det tapet de fikk siden de ikke fikk levert som de skulle. Også er det jo selvfølgelig det å få rekonstruert dataene. Også er det jo ekstra utgiften, de engasjerte jo, jeg mener det var Deloitte, det er jeg ikke helt sikkert på, det kan man jo google seg frem til. De jobbet jo på dette, jeg tror hvertfall et år, flere hundre konsulenter. De tre er de store utgiftspostene; driftstapet, ekstra utgiftene og denne rekonstruksjonen av data. Også selvfølgelig de hadde jo ganske uflaks, det var jo en server i Ukraina eller noe sånt noe som ble hacket, vi en underleverandør. Så spørsmålet er jo hvor mye du kan gardere deg mot det i fremtiden, det vet jeg ikke. Men det er jo sikkert en del kostnader forbundet med det å vurdere IT sikkerheten sin, og hvilket tiltak de skal gjøre. Mats [00:31:16]: Ja, for jeg leste at de hadde en server i et land i Afrika, som var nede på grunn av strømbrudd, så da fikk de reddet all informasjonen sin fra før angrepet. Så de fikk det tilbake til København. Så det var egentlig det som gjorde at de klarte å være oppe å gå igjen etter to uker. Så da kunne de rekonstruere det. Så de hadde jo

		flaks i uflaksen. Ellers så hadde tapt flere ganger det de tapte, anslåtte de. Kris [00:31:50]: Det er jo et sinnsykt kult case, men jeg ble så nervøs for informasjonen, tilgangen til informasjonen. Hvis vi skal ta case angående økonomiske konsekvenser, må vi få tilgang til Maersk sine poliser. Eirik [00:32:06]: Har dere prøvd å kontakte dem? Kris [00:32:12]: Nei, vi må først etablere med deg, få litt informasjon der, og når vi først kommer oss inn i det tar vi kontakt. Mats [00:32:19]: Men Morten har sagt at informasjon, burde vi klare å få tak i. Men om det er den vi helst ønsker oss, gjenstår å se.
	Emerging market	Eirik [00:32:29]: Men i Norge så er det et veldig umodent marked, og forsikringsselskapene, sånn som meg da, jeg jobber med all næringslivsforsikring, eller altså bygninger, eiendeler, driftstap og ansvarsforsikring, også har vi jo fått cf. Men det utgjør enda en veldig veldig liten del av porteføljen. Enn så lenge er det ikke brukt enorme ressurser på dette enda, men det kommer til å komme mer og mer i alle disse forsikringsselskapene, fordi kundene etterspør det mer også. Mats [00:33:04]: Men mye av verdien i Norske selskaper ligger vel nå i kunnskap og kundeinformasjon Eirik [00:33:11]: Ja det er jo mye av det, og det er jo datainnbrudd. Også er det spørsmål for fremtiden, man kunne jo spurt om hvorfor dette bare ikke er dekket på en annen forsikring, hvorfor må man ha en egen cf, og det ligger i at det er slik reassuranse har organisert seg, så i dag er det egne reassuranse for datainnbrudd. Men det også er jo et spørsmål hvordan det skal løse i reassuranse markedet i fremtiden. For det er en utvikling der om hvor den risikoen skal være dekket. Blant annet hvis det skjer et datainnbrudd som gjør at en bygning brenner for eksempel, hvor er det dekket? Det er en del sånne spørsmål som er uklare i reassuransemarkedet. Det er en ny risiko for hele forsikringsmarkedet egentlig. Også har man en cf som dekker datainnbrudd, med nedetid og

		rekonstruksjon, men det kan jo skje en del andre følger av et datainnbrudd. Fysisk skade, bygget her kan jo i prinsippet brenne ned, og hva da, hvis årsaken er datainnbrudd? Det er en del sånne ting som er litt uklare. Mats [00:34:30]: Så det er mangler på eksempler og tidligere hendelser? Eirik [00:34:35]: Ja. Men så er det jo sånn at i Gjensidige så hadde man data kriminalitetsforsikring, som de begynte med i 1999, og da også var det veldig sånn at dette er det nye store, om 20 år selger vi mer av dette her enn vi selger brann forsikring. Og da var det ikke måte på hvor stort dette skulle bli, men da kom det for tidlig, så det tok jo aldri helt av. Så man får jo vente å se, hvor stort dette her faktisk blir, men verden blir jo mer og mer digitalisert, så mye skulle jo tilsi at det på et eller annet tidspunkt, så må det være et større marked for cf enn det det har vært frem til nå. Kris [00:35:25]: Ja, det er jo hendelser, som med Hydro, plutselig fikk du mer henvendelser og det er de kjempe hendelsene som gir den awareness. Eirik [00:35:33]: Veldig, enn så lenge, i hvertfall generelt så vil jeg påstå at det jo for de store kundene dette er et stort problem for. I SMB markedet som er 99% av selskapene i Norge, for noen av de er dette en veldig stor risiko, men for de aller fleste så er det andre måter å gardere seg på en å kjøpe cf. Du har anti virus program, ha beredskap hvis det skulle skje noe, ha backup. Det er mange måter å gardere seg for den risikoen, hvor cf er en av de. For de store virksomhetene, som kanskje har behov for å risiko avlaste, hvis de skulle få en stor utgift. Så man får jo se hvor stort dette blir. Men jeg skal få se hva jeg kan få frem av en polise. Mats [00:36:31]: Det hadde vært helt supert. Kris [00:36:35]: Men det er fantastisk det, tusen hjertelig takk for all info. Vi hadde jo egentlig flere spørsmål, men du dekket jo alt gjennom prate. Så prima det Eirik [00:36:45]: Så bra. Hvis dere har noen spørsmål er det bare å sende noen oppfølgingsspørsmål, eller selvfølgelig bare å ringe også.
	Mainly for large companies	

Appendix A2 – Transcription and Analysis of Interview with Nanna Unhammer 04.02.20

Semantic Codes	Latent Codes	Transcription of Interview
	Influence of Changing market conditions	[00:00:01] Nanna: Nei, hvis du tenker på forsikring generelt da, hvis du går litt tilbake i historien, så startet jo forsikring egentlig med at Loyds forsikret skip. Et skip som gikk ned, varer som gikk tapt, altså en fysisk hendelse som førte til en fysisk skade, ikke sant, en ren konkret konsekvens. Også har jo forsikring utviklet seg den har jo flyttet fra hav over til land, hvor man har brannforsikring, hvis et hus brenner ned, det var jo det det begynte med på land. Hus som brant ned, du trenger å dekke det, for kostnaden ved å bygge opp et helt hus er såpass mye at det er vanskelig å sitte på den eksponeringen alene. også har man sakte men sikkert dratt det litt lengre. fordi at utgangspunktet for forsikring har vært en fysisk hendelse med en konkret fysisk konsekvens. også har man jo fått bygd på slike type forsikringer ved at man også har avbruddstap. altså du har en bedrift som har en brann, du skal dekke oppbyggingen av selve bedriften, men i tillegg det økonomiske tapet man har på grunn av at man ikke kan produsere i den tiden, så det er et konsekvens tap av brannen. sånn at du strekker begrepet fra det rent konkrete til litt mer konsekvens. Problemstillingen rundt cyber har jo vært at mye av det som defineres rundt cyber dekkes ikke av tradisjonelle forsikringer på mange måter, fordi at tradisjonell forsikring krever en fysisk hendelse, cyber defineres ikke som en fysisk hendelse, derfor får du ikke det vi kaller triggeren, den er da ikke oppfylt, så hvis du har hatt en cyber hendelse som fører til en fysisk hendelse, så har du fremdeles i de tradisjonelle forsikringene gjerne en dekning. det kommer vi tilbake til for der begynner det jo å skje ting også. så si at du har en cyber hendelse som fører til en brann, så har du i utgangspunktet de gamle forsikringene, for da har triggeren blitt oppfylt, du har en brann som er en fysisk trigger. Men det som cyber gjerne kan føre til er jo at systemene dine går ned, du får ikke gjort noe, men det er ingen fysisk skade. du er bare lammet, fordi at du ikke har noen fysisk trigger, så er det egentlig ingen forsikring som har

	Lack of data	plukket opp, du sitter egentlig mellom barken og veden, og det er jo der egentlig cf har kommet inn, for de har sett på at okey, du har ingen fysisk hendelse, vi må lage en trigger, som på en måte passer dette her, for det er egentlig ikke noe produkt innenfor dette her. Jeg vet ikke hvor godt dere kjenner forsikring, men du har begrepene; førsteparts- og tredjeparts tap. **[00:02:50] Mats: ja det har vi vært borti** [00:02:49] Nanna: Første part er jo på en måte kundens eget tap, som du lider, tredjepart er det tapet du kan påføre en annen. og innen tradisjonell forsikring så sier vi at ting skade er førsteparts tapet mye, ting og avbrudd. også har du ansvar som er overfor tredjepart. ansvarsforsikring har også vært hengt på det fysiske, det skal være fysisk ting- eller person skade. Det har vært triggeren, så igjen der så har du ikke hatt en trigger som kan plukke opp de andre. nå finns det utvidelser innenfor ansvarsforsikring som heter rent formuestap, som plukker opp noe av dette, men det som har vært noe av problemstillingen, er jo at de aldri har hatt cyber hendelser i tankene forsikringsselskapene. Og det er noe av problemstillingen som vi også ser nå, at hvis du har en cyber hendelser som trigger en brann så har jo de tradisjonelle forsikringen i utgangspunktet plukket det opp, men nå begynner vi å få unntak, mann begynner å se på det, fordi man har aldri vurdert den risikoen, de har ikke tatt hensyn til det når de har underwriter risikoen, så har de på en måte sett på de tradisjonelle eksponerings problematikken og ikke cybern. og der får vi jo litt problemer, for cf er egentlig bare ment å dekke det rent økonomiske tapet. sånn at hvis du får en cyber hendelse, som fører til en brann og du får ett unntak på brannforsikringen din, for en cyber hendelse, så har du et problem igjen. så det er mye av det som bransjen jobber med nå, de må på en måte lære seg hva den eksponeringen medfører, også har mann fått, og det her begynte i England, der myndighetene rett og slett satt krav til forsikringsselskapene at man ikke skal ha silent cover. Det var jo det man hadde tidligere, der en brannforsikring plukket opp en brann som følge av en cyber hendelse. Det var ingen unntak og det var ikke spesifisert og da kaller man det silent

	Influence of regulations	cover. Forsikringsselskapene, ble jo pålagt at de enten måtte eksplisitt ta det inn, eller eksplisitt, ta det ut. Og da selvfølgelig den enkleste måten er jo å ta det ut. for det å ta det eksplisitt inn betyr jo at man må vise at underwriter det, at du har vurdert den risikoen. [00:05:15] Erik: Og, på kjøper side som en kostnad. og der det vel kanskje, mye av kjernen på problemet, kundene vil jo stille spørsmål ved dette her. Det har jo vært implisitt dekket tidligere, hvorfor skal man nå begynne å betale ekstra for en risiko som dere allerede har påtatt dere i årevis, men den risikoen har ikke (forsikringsselskapene) påtatt seg i årevis. For risikoen er eksponentielt økende. [00:05:39] Nanna: Det er jo litt det samme som at når det kommer nye risiko elementer, vi ser jo blant annet innenfor, naturskade, der vi på en måte får flere katastrofer som gjør at noen områder får høyere premium for vi ser at eksponeringen der er høyere enn det den har vært tidligere. Kostnaden ved å dekke den typen forsikring. Hvis du tenker "tradisjonell" cf, det er jo relativt nytt, men altså det som man tenker som cf, er ment å dekke det rene økonomiske tapet. det er tre elementer; Inntektstapet som følge av nedetid, håndteringen av hendelsen, noe det Maersk hadde mye problemer med, de hadde jo ikke forsikring, har det nå. Men de måtte jo leie inn mangfoldige konsulenter, altså de hadde et helt bygning stående i London som de bare fylte opp med IT konsulenter, de kjøpte inn alt av bærbare pcer de kunne kommer over, bare det er en vanvittig kostnad. Og de har jo fremdeles faktisk konsulenter jobbene hos seg. **[00:06:50] Kris: Ja, vi så Deloitte hadde over 100 konsulenter, og det var jo hele spekteret, det var ikke bare IT konsulenter der, det var jo alt.** [00:06:57] Nanna: Så, ikke sant, du ser jo den kostnaden drar jo veldig på. så for cf tanken bak det er at den skal hjelpe deg å dekke den kostnaden som du får ved en slik hendelse. og det er jo førsteparts kostnad, ditt tap. Også er det også i forhold til cyber extortion, det er egentlig bare utpressing. Og der er det også veldig mye diskusjoner rundt, hvorvidt forsikringsselskapene
	Changing market conditions	

Coverage of CF Role of CF	Influence of regulations	sier at de dekker utpressings beløpet, så sant det er lovlig. Og der kan det jo være diskusjon, det gjelder jo også på tredjepart i forhold til GDPR. Der har det vært veldig mye debatt rundt om den boten (GDPR boten) er lov til å dekke. som vi sier til kundene så bør man ha en forsikring som sier at den dekker lovlige bøter. Vi vet jo ikke per i dag om det blir lovlig, myndighetene sine indikasjoner er jo det hvis det skal bli mulig å forsikre seg bort, så blir jo hensikten med boten, den faller jo bort. Og datatilsynet har jo satt at de i utgangspunktet ikke ønsker å gi den boten, med mindre det er alvorlige brudd. og da blir det også helt meningsløst. I Norge har vi innført EU lovgivning egentlig strengere enn noe annet land tidligere, også skal vi plutselig bli en frihavn, virker meget usannsynlig. Grunnen til at jeg tror at de (dle piper) har tolket det på den måten, er fordi at GDPR lovgivningen har vært håndtert under sivilrettslige regler i Norge, hadde det vært håndtert under strafferettslige regler så hadde det vært forbudt. Nå skal det sies at bøter i fra myndigheter stort sett alltid blir sett på som straff, og dermed er det usannsynlig. Men videre, bort i fra det så er det at de kravene likevel i forhold til tredjepart, en ting er jo i forhold til GDPR og personopplysninger, men du kan jo sitte på bedriftsinformasjon, som kan føre til at de kan ta penger, så igjen men da må man jo være rettslig erstatningspliktig, du må på en måte ha utlyst en eller annen form for skyld. Du må kunne legges til last for dette her. Men da er det jo den dekningen, og det gjelder både notification, i forhold til oppfølging, kanskje monitorering av informasjon som har kommet på avveie, alt dette medfører jo kostnader for deg som selskap. som cf dekker, men igjen alle elementene her er rene økonomiske elementer, det er ikke ment til å dekke, si at du håndterer lyskryss også er det noen som går inn å leker med det, slik at alle får grønt samtidig, også får du en stor kollisjon. [00:09:46] Mats: Rykte og den delen da? [00:09:51] Nanna: Nei, ryktet, hvis du tenker medier, det kan dekkes under cf, hvis noen legger ut noe på internett, for eksempel, så kan du kreve det dekket. men her tenker jeg hvis det er noen som leker med lyssignalene slik at et to tog går mot hverandre eller at lyskryss blir grønne slik at man krasjer, så får man en fysisk skade. Cf er ikke

Coverage of CF Role of CF	Potential for damage	ment til å dekke den fysiske skaden. og derfor er det jo veldig viktig at man følger med på de andre forsikringene også. og det har vi prøvd å snakke litt om, hvis du tenker deg cyber (tegner på tavlen) cyber er en svær sky også har du mange forsikringer inne i den skyen, du har GLPL som er ansvar, du har PDBI som er ting og avbrudd, du har auto forsikring, alle disse her er eksponert for cyber risikoen, fordi at data er en del av hverdagen vår på alle kanter, vi er helt avhengig av det, sånn at du kan på en måte ikke sidestille cyber eksponering og cf, for cf tar en liten del av det. men hvorfor er cf så viktig? det er jo det vi har sett hos Maersk, den enorme kostnaden det her kan medføre en virksomhet. Det er klart at det vil påvirke konkurransesituasjonen til selskapet, kan man i det hele tatt overleve? En ting er jo disse veldig store virksomhetene, som Maersk og Hydro, som har ressurser å putte inn i dette her, og som har muligheten og som er så store at det ikke bare er å bytte de ut. Men hvis man tenker på litt mindre virksomheter mellomstore, tenk på de nettvirksomheten, hvor lojal er du mot elkjøp eller power eller noen av disse her. Hvis den siden er nede så snur du deg bare rundt og finner en annen som selger samme type produkt. lojaliteten din er null. de virksomhetene er kjempe påvirket, fordi at du har ikke noen relasjon til den virksomheten som sådan. du skal bare ha et produkt, så når de får nedetid så er det viktig for de å ha muligheten til å komme raskt opp igjen, ha muligheten til å få bistand til å både kanskje gå ut i media og å informere, og til å gi muligheten til goodwill cupon som man kan få dekket, rett og slett at man kjøper tilbake kundene sine. Man kan sende ut mail til hele kundemassen, og si ok hvis dere kommer tilbake og kjøper noe nå, så får dere så og så mye rabatt, eller noe lignende. Det er rett og slett der for å minske sjansen for at du mister kundene dine på sikt. Det er jo rett og slett det å beskytte bunnlinja, beskytte levegrunnlaget til virksomheten, det er det cf skal være med å bistå til. Du får jo ikke dekket alt, men du får på en måte sikret mye av problemstillingen rundt det. **[00:12:50] Mats: Immaterielle verdier og sånn, patenter?** [00:12:54] Nanna: Patenter er et generelt unntak. men man har stort sett en carveback for forretningshemmeligheter, det kommer litt ann på.

		Men patenter der finnes det egne forsikringer, man har IPR (intellectual property rights) forsikring som er ment å dekke det, og det er igjen, forsikringsbransjen prøver å dele opp, på en måte spesifisere dekningen, det er jo også i forhold til cyber at mange tror også at cyber dekker underslag som har foregått via cyber, det er det jo ikke ment til å gjøre. Du kan få en liten forsikringssum, men det er ment dekket under kriminalitetsforsikring som igjen er et annet produkt. forsikringsselskapene prøver å avgrense områdene og det er litt for å kunne kvantifisere risikoen, det er veldig vanskelig når du skal putte veldig mye inn i samme "boks" **[00:13:47] Kris: Hvordan takler dere tvetydigheten, for vi så jo blant annet den Mondelez saken?** [00:13:53] Nanna: Ja, og mondelez saken er jo ikke en cf sak. Der var det jo Zurich som avslo i utgangspunktet, men den saken er vel ikke helt avgjort enda, for den skal vel opp i rettsvesenet, men de avslo ting forsikringsdekningen, altså de hadde hatt et inntektstap, jeg husker ikke helt hva det var, men det var ting forsikring det gikk på, og de avslo saken ved å bruke krigs unntaket, de mente at det var på grunn av Russland-Ukraina situasjonen. Nå tror jeg veldig mange i bransjen, om Zurich vill få støtte i sin tolkning av det. Innenfor cf så er krigs risikoen definert litt annerledes. Du har fremdeles krigs unntak, men du har en carveback for cyber terror, altså hvis det er en ren cyber hendelse så vil du få dekning for det. Så Mondelez saken ville neppet vært unntatt, vi har jo hatt andre lignende krav, under cf relatert til NotPetya og disse her som har vært dekket. Så cf oppfører seg litt annerledes enn den tradisjonelle. Men igjen så er det den problemstillingen som jeg snakket om i begynnelsen, under den tradisjonelle forsikringen så har man ikke tatt høyde for cyber risikoen. og det er cyber risikoen som har trigget mondelez saken, men det er ting forsikringen som er ment å plukke det opp. Zurich har aldri vurdert den delen av risikoen mest sannsynlig, det er det som gjør at de sitter og er ukomfortable med det. For under en tradisjonell ting forsikring så ser du på for eksempel de ulike verdiene som blir rapportert inn, og hvor de er plassert hen, slik at du gjør en kumule vurdering, hvor stor er risikoen vår på

	Pricing and risk assesement	dette område. På en tradisjonell brannforsikring, så brenner det i det området og den brannen kan spre seg sånn ca., man klarer å gjøre en beregning, problemstillingen for cyber er at den kan slå ut like mye i Finnmark som i Singapor, du har ikke den begrensingen, det gjør det mye vanskeligere for forsikringsselskapene å bergene kumule risken sin. **[00:16:10] Kris: Ja, ikke sant du får jo ikke diversifisert risikoen, når den ikke er begrenset geografisk...** [00:16:17] Nanna: Ja, og du har veldig stor sjanse for at, hvis du skjer innenfor IT, så brukes mange av de samme selskapene; Amazon, Microsoft ikke sant SRP, mange av disse samme selskapene går igjen hos mange kunder, så si at SRP som innenfor produksjon blir rammet, så kan jo potensielt alle SRP kunder bli rammet, da får man en kjempe kumule. **[00:16:40] Mats: Hvordan, hvis de har vansker med å beregne risikoen, hva gjør de da?**
	Lack of data Influence of subcontractors Demands put on customers	[00:16:47] Nanna: Det de har gjort i stor grad, og som de prøver å jobbe med, er å begrense kapasiteten de tilbyr. De kan gjerne på f.eks. ting forsikring tilby milliarder i forsikringssum, mens på cyber så tilbyr 100 millioner. Så de begrenser det ved å ta det ned, samtidig prøver de å kartlegge, for i begynnelse var de ikke like flinke på det, nå er de veldig nøye på å kartlegge hva slags leverandører de ulike kundene bruker, for å prøve å lage en sånn mapping av det. **[00:17:18] Mats: Ja, av IT nettverket?** [00:17:22] Nanna: Ja, du vil vite hvilke leverandører bruker du, hva slags systemer. Slik at du på en måte vet. Er det en sånn typisk Microsoft ting så vil det slå ut på alle som har Microsoft, hvilket er veldig mange. Men så er det jo det at alle systemer henger jo ikke sammen heller. Det er viktig for forsikringsselskapene å vite hvordan systemene er segregert og vi ser jo det når vi plasserer cyber. I begynnelsen var det en del spørsmål rundt generelle ting, også var det noen IT relevante spørsmål, nå er de blitt veldig nøye på å gå i dybden, de vil vite hvordan jobber dere strategisk, hvordan segregerer dere

	Lack of data Emerging market	systemene, har dere OT og IT systemer, hvordan jobber dere med det. Veldig nøye for å kunne skape seg et bilde modenhet til virksomheten. Så det krever veldig mye informasjon. **[00:18:11] Kris: Men samtidig som den trenden at de begynner å kartlegge, har dere sett noen trend i premiumene, om de har steget mens risikoen har sunket (eller vice versa)?** [00:18:20] Nanna: Ja, det har vi sett, veldig tydelig. Vi hadde for noen år siden så var det blant annet Munich RE og Bisley kombinert, de tilbød 50 millioner i limit, per 01.01.20, så har de oppløst sitt samarbeid, vil ikke gå ut å tilby så mye, jeg vet fremdeles at Bisley og Munich RE er noen av de som tilbyr mer kapasitet enn de andre. AIG som har vært en av de virkelig store aktørene, de tilbød jo egentlig 25 og kunne potensielt tilby mer, de har gått ned til, altså nå snakker vi millioner euro, de har gått ned til 10. De har redusert alt. de går ned på alt. Tidligere kunne vi lage større forsikringsprogrammer, med store kapasiteter, det får vi ikke til nå. Nå får du stort sett små kapasiteter, så du må ha mange aktører med for å få dekket opp store summer da. Så si hvis du skal ha en milliard NOK så må du ha 10 aktører omtrent for å få det til, mens før kunne du kanskje klare deg med 5-6. **[00:19:26] Kris: Ja, du klarer kanskje ikke å kommentere noe for Hydro, men de bruker jo den Captive sin, og da er det kanskje lettere å gå rett inn reassuransemarkedet.** [00:19:34] Nanna: Ja, jeg tror vi skal snakke, det vi ser er at de som har captive, for vi har flere kunder som bruker captive. Er det at de bruker captive sitt som en reassuranse på cyber fordi at når man bruker captive så er det jo under forutsetninger om at man har kunnskapen om det markedet. Og de tradisjonelle forsikringene som ting, avbrudd og ansvar det kan man nokså godt, man har lang historie, man har modellerings modeller rundt dette. Slik at captivet lettere kan ta det selv. På nye risikoer ser vi veldig få gå inn på direkte siden på cyber, de stiller seg egentlig bak som en reassuranse kapasitet selv. Så de velger for eksempel å bruke en av de store som har erfaring; AIG, Chubb, QB, AX... en eller annen av disse her, som front. Også sier de av at av den

SMBs lagging behind	Lack of data	primær dekningen dere tar så tar vi en andel, så vi tar den nederste delen, slik at det blir en slags egenandel struktur inne i dette her. Men de ligger veldig sjeldent i front, og det har med erfaring å gjøre. [00:20:46] Erik: Bare i tilfelle, du sier dette så veldig veldig bra Nanna, men i tilfelle det er ikke store forskjellen her mellom reassuranse markedets oppfatning av risiko og risikovurdering, og direkte markedets. Disse tingene henger veldig veldig sammen, og mye av den kapasiteten som er tilgjengelig drives jo fra baksiden, fra de gutta som sitter her (peker på reassuranse på tegningen på tavlen) det er Munich, Bisley og det er Swiss ikke sant. Men der får dere (PP på overhead) i hvert fall en liten ide om hvordan man forventer at premium nivået kommer til å stige i løpet av årene, og dette her er jo produkter som er under konstant utvikling, risikobildet er under konstant evaluering og re-evaluering slik at det dere ser i premium størrelse i 2025 er basert på en helt annen virkelighetsoppfatning enn hvordan den er i 2020 eller 2015, for den slags skyld. Men det sier litt om suget i markedet, behovet som har oppstått, og siste punktet der er også veldig interessant, det plukker opp eksakt det du sa Nanna, nemlig det at reassurandørene er mer og mer oppmerksom på kumule problematikken her. På smitte problematikken, og det begrenser risiko apetitten naturligvis også.
	Emerging market	
	Role of reinsurance	
	Emerging market	[00:22:03] Nanna: Jeg er helt enig med den forecast som Erik har tatt opp her, for det vi ser er, bare nå fremdeles så er det få som kjøper cyber i forhold til de som kjøper det mer tradisjonelle. De fleste store norske tror jeg enten er i prosess eller har kjøpt. Willis Norge sitter jo på veldig mange av de og vi er i prosess med de fleste, men fremdeles så ser vi at smb markedet ikke helt har catchet opp enda, og jeg mener jo at der er de mest sårbare. Erik [00:22:44]: De pluss kommunene og fylkeskommune, det vil jeg påstå. Å sitte i dag og være rådmann i en stor kommune, med en enorm økonomisk eksponering, og ikke kjøpe cyber jeg skjønner ikke at de tør jeg.

		Mats [00:23:03]: Man så jo bare den saken i Bergen, med han 13 åringen eller hva det var. Kris [00:23:06]: Ja de sitter på så mye personopplysninger. Nanna [00:23:09]: Ja, det er jo det de gjør, vi kategoriserer personopplysninger i tre bolker, du har PI, som er Personal Identifiable information, PCI, som er Personal Credit Information, hvilket som stort sett er finansielle institusjoner. Også har du PHI, som er helseinformasjon, kommuner, fylkeskommuner, sykehus alle disse her sitter med veldig mye av det siste (PHI). sånn at det er klart at du har et veldig stort krav, og Bergen fylkeskommune fikk jo en bot, ikke sant. Men den premium utviklingen som Erik har tatt opp her, den tror jeg at er veldig illustrativ. egentlig så hadde det vært litt interessant å sett det sammenlignet med property premien. Fordi at ting og avbruddsforsikring har vært litt sånn typisk produkt som det har vært veldig fokus på, fordi det er så store premium volum. Det er store verdier og store premium, det er et modent marked. Men hvis du tenker deg en virksomhet som har en ting og avbruddsforsikring, får du en ting skade, så er det stort sett på en site. Får du slik som Hydro en cyber hendelse, så slår det ikke ut en site, det slår i utgangspunktet ut alle. Så depending on how many sites you have så kan det jo bli kjempe svært. Jeg tror jo at avbrudds risikoen på cyber, altså den rene avbrudds risikoen der, vil øke. Altså det vil eksplodere fremover, jeg tror vi kan se konkurrering mot pvbi premien.
Coverage of cyber	Potential for damage	Erik [00:24:41]: Er dere kjent med begrepet CBI, contingency business interruption? Det er et avbruddstap på et sted som selv ikke har opplevd skade. Vi kan se dette for oss i cyber veldig veldig klart. Nanna [00:24:58]: Vi har CBI dekning, man foretrekker å tegne cyber på konsern nivå, også har man stort sett et unntak, innenfor ansvar så har man noe som kalles cross liability, altså det vil si at selskap innenfor samme konsern kan være ansvarlig overfor hverandre. I cyber så er det unntatt, man får ikke en cross liability der. Men hvis du tegner konsern dekning, så vil jo de som er påvirket, være dekket uavhengig. Innenfor cyber så har du contingent business i forhold til IT

		leverandører, så du får dekket tap hos deg, hvis dine it leverandører har en hendelse. Men det er en utvidelse. Erik [00:25:39]: Men vi kan se for oss en bedrift som er leverandør av viktige komponenter til en annen bedrift som igjen er en stor leverandør til for eksempel oljeindustrien. Her er det en link hvis det da oppstår en hendelse i bedriften som er underleverandør. Nanna [00:25:57]: Da har du jo mye problematikk rundt kontrakts ansvar, for det er jo vanlig med unntak, for rent kontraktsansvar. Du vil dekke ansvar som du ville hatt i fravær av kontrakt, men ikke et utvidet kontraktsansvar. Og late delivery og sånn, sorry det er en business risk, så det får du jo ikke dekket. Også er det jo igjen hva slags type krav fra tredje tap vil du kunne få dekket. Du vil jo ikke få dekket fysisk ting- og personskade hos tredjepart. Så hvis din leveranse fører til en annen skade hos de, annet enn rent økonomisk, så er det jo ikke cyber som er ment å plukke det opp. Så grensedragningen er jo litt ulne.
	Emerging market	Erik [00:26:44]: Det er et godt stykke igjen å gå. og jeg opplever i hvert fall i min verden, avhengig av hvem jeg snakker med, så er oppfatningen av cyber risiko og cyber utfordringer forskjellig. Folk tolker ulike ting inn i det begrepet. Nanna [00:26:58]: Men vi ser en veldig modenhet hos virksomhetene, for når jeg begynte å jobbe med dette her for en seks år siden, så var det omtrent som å løpe med hodet inn i en vegg, fordi alle synes det er kjempe morsomt å høre på, ingen var interessert i å gjøre noe. Og hvis du snakket med IT avdelingene, så var det; jammen dette har vi kontroll på, ikke kom å stille spørsmålstegn ved dette her, vi kan jobben vår. Også er det jo sånn at du kjøper jo ikke en bilforsikring fordi du har tenkt til å krasje. Det er jo ikke derfor du kjøper forsikring det er jo i tilfelle det skjer. og det er jo akkurat det med cybern og der ser vi en veldig endring hos it avdelingen, de ser på oss som en støtte, altså dette her er noe som er ment til å supportere den jobben vi gjør i hverdagen. blant annet med at det dekker it konsulenter. Også har vi kunder som går under NSM, som ikke kan ta inn eksterne, men de eksterne kan kanskje brukes til å sørge for andre typer drifting av

	Professional support	virksomheten, hjelpe å supportere dere (virksomhet) på andre områder, mens dere selv konsentrerer dere om de sensitive områdene. sånn at forsikringen er ment å være en støtte i en hendelse. Hvilket er litt annerledes enn mange av de andre forsikringene som kommer inn etter faktum er på plass, også skal du egentlig bare betale ut. Og det er også en av de tingene som er viktig med cf er at den skal trigges ikke bare når du vet du har en hendelse, men også ved mistanke om en hendelse så kan man trigge forsikringen, man kan få inn støtte allerede for å få avdekket om det faktisk er noe. Si at du kommer på jobb også oppdager du at pcene oppfører seg litt merkelig, og da kan du i utgangspunktet ringe. Og da er det jo klart at for store virksomheter som har profesjonelle it avdelinger så kan de kanskje gjøre mye av den jobben selv, men for mellomstore bedrifter så koster det veldig mye å kanskje ha et firma stående eller å ha tilgang til det. Da kan de bruke forsikringen til å få tilgang på riktige ressurser, til å få avdekket om de faktisk har en hendelse. **Kris [00:29:10]: Jeg tenkte jo også på det falsk angrep opplegget, der hvis man har forsikringen, så vil jo ikke forsikringsselskapet at de skal vente helt til det slår ut noe, men heller tar de den kostnad først, i tilfelle det ikke er et falsk angrep.**
	Professional support	Nanna [00:29:24]: For du har jo en egenandel, men viser jo også at noen forsikringsselskaper tilbyr noe som heter first response eller emergency response, og det vil si at de går inn og dekker de første 12, 24, 72 timene, og da kan du ringe en hotline, du har fri tilgang på konsulentbistand gratis i de første timene, for å avdekke om dette er noe. Og det er igjen for å oppmuntre kundene til å faktisk bruke forsikringen, også vet du at etter den perioden, så utarbeider man en rapport, også sier vi at dette her mest sannsynlig er ingenting. Da kan kunden velge om de skal gå videre med saken selv. Eller ja dette her er mest sannsynlig en hendelse, da kan de velge om de vil trigge forsikringen, for de første timene er det ingen egenandel. Og det er igjen for å få det fort inn i systemet for å få det i gang. For de absolutt største så ser vi at den type dekning kanskje ikke har vært så viktig, fordi de har et helt annet type apparat, de har ofte

	Pricing and risk assesement	selskaper som driver monitorering for de, som gjør en del av den jobben, men SMB markedet ikke har den type ressurser. **30:47** **Rapport fra Deloitte, leste om de skjulte kostnadene, tilgang på polis fra gjensidige og om de får støtte fra reassuransemarkedet.** Ja det får de nok. **Hvertfall da hadde ikke dekning for kapitalkostnader, så i så fall om 1,2,3 år og rentekostnader på obligasjoner og etc.** Det er stort sett et unntak, det er og sånn i forhold til at man har ofte mange slike tradisjonelle unntak. Gjensidige er ikke det jeg ville kalle (uten å være slem mot gjensidige) det jeg ville brukt, men du vil se at det er en del slike kostnader som tas bort og i forhold til tap av konkurransefortrinn. Du får dekket inntektstapet i denne perioden og du kan få bistand til å komme tilbake, men andre ting som også påvirker vil også bli trukket i fra. Jeg vet ikke om dere kjenner til avbrudd beregningen men det er veldig.. ting forsikring er latterlig enkelt, mens avbrudds beregning er latterlig komplisert, fordi at man skal beregne hvor mye inntekten til en virksomhet har vært i en periode og så skal man ta høyde for andre påvirkninger, markedspåvirkninger, uventet hendelsene og alt dette skal spille inn og gjør det veldig komplisert og det er ikke noe mindre komplisert med cyber! det som har vært forskjell mellom ting avbrudd og cyber avbrudd er at perioden har vært mye kortere, som dere så med Maersk, de var nede en kort periode, men tapet ble veldig stort. Med ting forsikring kan avbruddet være i opptil 36 måneder, mens på cyber har det vært 180 dager. Det har noe jeg tror har begrenset premium utviklingen, men nå ser vi at flere selskaper går utover det og tenker mer som de tenker med ting forsikringen. At man skal dekke det tapet som følger av hendelsen, om det er 180 dager eller om det er mer som må tilpasset, da må man naturligvis få en høyere premium også. Fordi det blir et større tap som vil falle inn under dekningen. 33:51 **Men du snakket om at de må lære seg eksponeringen underveis**

	Lack of data	Fordi ja, man har ikke sett hvordan det faktisk fungerer i praksis. Det ser man jo nå med hydro, man ser det maersk og ser hvordan effekten av en hendelsen faktisk kan påvirke bedriften. **Så man sitter egentlig og venter på hendelser?** Ja man prøver å lage scenarios, hvis det skjer, det er veldig typisk ting man gjør og det gjør man for tingforsikring også. Man lager seg et estimated maximum loss scenario. Hvis det skjer, hvordan vil det potensielt, og hva vil hvis man setter inn disse tiltakene kunne redusere risikoen problemstilling er at på tingforsikring har man så mye erfaring og historisk data å trekke på og vet hvordan forskjellige ting spiller mot hverandre, mens det har man ikke på cyber! Man har ikke kartlagt det tidligere så man mangler den historiske dataen og det skal sies forsikring er veldige sirumpa. De vil jo gjerne vite og det gjør at man sitter gjerne litt tilbake og ser ok, hva skjer, hvordan vil dette utspille seg. Det gjør jo at produktet i seg selv, selv om vi ser en utvikling, ser vi at det ikke er store endringer i selve hva de tilbyr, men gjerne heller justering i premium, i de mindre tingene etterhvert hvordan de ser at det faktisk påvirker. **Nå har vi jo nevnt de forskjellige problemstillingene, hvorhen det ene vi så på var å se på endring på cyber forsikringsmarkedet ut fra de forskjellige angrepene hvor vi primært så for oss maersk, equifax og hydro. Vi lurte dermed ang. hydro/maersk hendelsene, har dere opplevd flere henvendelser. Du nevnte/jobber med storkunde-markedet..** **36:35** Jeg jobber bare med storkunde-markedet. Og det morsomme er at jeg var i London 19. Mars i fjor, når Hydro hadde sitt angrep og jeg har jobbet med dette i en del år nå. Og har vært i kontakt med mange kunder. Sånn ca. utpå ettermiddagen den 19. Mars, så sto i tlf. Da ringte alle de jeg hadde hatt møte med og.. "Du, du forresten husker du det møte, nå skal jeg ha forsikring." Så det er klart, Maersk-saken trigget interesse, men jeg er litt overrasket over lite interesse marin-markedet har vist

	Emerging market	**For det skulle man nesten tro, med tanke på hvor avhengig de er av løsninger som IoT** Spesielt med tanke på de innenfor skadeforsikring, da sier vi marine og non-marine, non-marine har hatt produkter som dekker det vi kaller pure-financial losses det har man hatt produkter for, marine-markedet har ikke hatt disse. Så de har kun fysiske hendelser, i all hovedsak dekket. Det de har noen tilfeller dekket seg bak, nå er jeg litt kritisk mot marine markedet, men det de har dekket seg rundt er war-dekningen for de mener de kan stappe en del av cyber-dekningen inn der. Noe kan de, men hva defineres som var, de fleste cyber hendelsene vil ikke defineres som var. Da kan man ikke trigge war-forsikringen. Sånn det med hydro, det er ikke en krigshendelse, det er et virus. Det er en eller annen organisasjon som har bestemt seg for å ramme produserende virksomhet. De utnytter svakheter i produksjonssystemet som de kjenner til. Det er klart at man da bruker systemet sitt i marine-industrien ser at det er noen klare svakheter som man ser man kan utnytte til egen-økonomisk vinning. Det kan ikke bli definert som en krigshendelse. Men jeg er litt overrasket, men det skal sies at marine-markedet er meget konservativt. Vi har møte med en del av de, men de henger fremdeles litt igjen. Jeg tror, merkelig nok, i hvertfall i Norge at Marine-markedet kommer også med sine egne cyber produkter, fremdeles tar det fryktelig lang tid. **Vi ser at norske markedet er veldig underutviklet på cyberforsikring. Selv i skandinavia.** Ja, Danmark og Sverige er mye lenger foran oss, men det interessante er at Sverige er som oss hvor det er mange av de store, mens Danmark er veldig flinke på SMB-markedet. De har klart å penetrere det markedet. Jeg vet ikke hvorfor, men jeg tror egentlig det er norsk naivitet. Hvorfor skal det skje oss, vi er ikke så viktige, vi er ikke så store. Selvfølgelig kan det skje de store, men vi er ikke sånn. Poenget er at man hadde frisøren på Kongsberg som ble hacket, de tok hele kundelisten. Det er klart for en liten bedrift går man konk.

		Vi så NotPetya, det traff ikke bare de store. Det var avdelinger i butikker i Norge som ble truffet.
	Damage potential	Ja, vi har jo veldig mye jobbet mye mot retail bransjen. En ting er butikkene i seg selv. Men hva skjer når de ikke kan imot betaling, når betalingssystemene blir slått ut eller logistikken. Du har store varelagre, f. eks asko. Hvis du slår ut systemet der. Hvis man slår ut systemet der kan det være som om varelageret er i teorien tomt selv om det er stappfulle hyller fordi de ikke kan sende ut noe som helst. Man har gjort seg så avhengige av teknologien. Det var en av fordelene til Hydro var at smelteverkene kunne opereres manuelt, men hva om 10-20 år da alle de som kan gjøre dette manuelt er borte, hva da? Tidligere har dette vært manuelt, men man har etterhvert gått over til teknologisk/digitalt styrt. Mye større konsekvenser når de som kan gjøre dette manuelt er borte. Dette er en avveining firmaet må tenke mye på, hva slags backup løsninger skal man. I forhold til en virksomhet man kan ha full data et sted og et annet sted, som er totalt like, men hva er kostnadene for å drive dette. Hva er kost/nytte effekten.
	Damage potential	**Det lurte jeg på ang. manuelt og Hydro, Falskt angrep** Dette er en dekning man kan ha, kalles Voluntarily shut-down. Hydro gjorde dette. De valgte å stenge alle systemene sine da de skjønte dette for å unngå potensiell spredning. Noen selskaper har unntak for dette mens andre har det med, men det er klart det er at gjelder i forhold til avbrudd at man ser på kost/nytte effekten. Det koster mye å ta det ned, mens kostnadene kan bli mye større ved ikke å ta det ned og det er skadereduserende tiltak. Det man ser er at innenfor avbruddsforsikring sier man ofte at ekstra kostnader så lenge det ikke overstiger det tapet som ville vært uten de så vil det dekkes. Men det er en vurdering man gjør, og en dialog mellom kunden og forsikringsselskapene. Og i dette tilfellet er det også it-konsulentene. Avbrudd er veldig komplisert, derfor leier man inn forensics accountants for å bidra til å gjøre vurderinger. For å si det sånn, konsulentbransjen de gjør mye penger på dette. De kommer inn og tilbyr sine tjenester i krisesituasjoner og kan i

	Demands put on customers Hard to understand the coverage	prinsipp ta hvilken pris de vil. Forsikringsselskapene kan derfor bidra til å drive ned disse kostnadene fordi de knytter til se et panel med pre-godkjente kostnader. Derfor kan man unngå den helt insane-faktureringen. Da kan man begrense kostnaden noe, og det er jo det forsikringsselskapene også er interessert i. 44:59 **Soderberg & partners analyse, mente at det var store forskjeller mellom forsikringsselskapers tilbud,** Jeg tror også det stemmer fordi nordiske lokale selskaper - stor variasjon mellom hva man får, gjensidige sitt, de er ikke en av de jeg godkjenner. Hvis en av våre meglere kommer til meg, nå har jeg fått tilbud fra gjensidige, sier jeg gå for et annet tilbud. Fordi de er veldig begrensende og de har mange sikkerhetsforskrifter som det er helt umulig for kunden å oppfylle. Man skal ha et godkjent virusprogram. Hva er det? Det står ikke definert hva det er for noe. Man skal ha profesjonelle brannmurer, igjen, hva definerer man som profesjonelle brannmurer. Produktet er veldig vanskelig for kunden å forstå. De har masse begrensninger og unntak. Nå jobber jeg med veldig store kunder, vant med internasjonale kunder med definerte vilkår og jeg mener at med cyberforsikring som er et såpass nytt produkt mener jeg at det bra siden det er så vanskelig å få hånd om hva man faktisk skal få dekket så det er bedre å ha tjukke vilkår som gjør det lettere å lese enn de veldige tynne hvor det er vanskelig å forstå intensjon bak dekning. **Tvetydigheten kommer fram da, hvor kunden kan tro noe er dekket, mens forsikringsselskapene mener noe helt annet.** Da sier gjensidige at står det ikke unntatt er det med. Ja, men det står ikke unntatt, men når det er skrevet i sikkerhetsforskriftene på den måten eller skrive unntak på den måten kan det tolkes inn og ut, det gjør at det er veldig utydelig for kundene. Den norske modellen om å skrive vilkår, alle kjenner til den lille skriften, men i Norge ønsker man å gjøre vilkårene veldig enkle, men akkurat for cyber tror jeg faktisk ikke det er en fordel, da tror jeg at større er bedre spesielt fordi man har en begrepsforvirring. Det er så mange nye begreper

		rundt hva er en security breach, hva er en privacy breach. Hva er det som egentlig ligger i begrepene. Det er ikke noe som er standardisert. Det er bedre å ha det skrevet ned. 46:43 **Begge partene har lite erfaring.**
	Process of standardisation	Ja det er nettopp det. Blant de store internasjonale syntes jeg at det begynner å se veldig at de går i samme retningen, de samme dekningene, litt forskjellige formulert. men i det store og hele er det er en standardisering rundt det hele. 47:24 **Har dere tilgang til forsikringspoliser/vilkår...** - Prates om tilgang til poliser og om hvordan hun generelt endrer vilkårene for å tilpasses de ulike kundene ..... **De Polisene, du får de standardvilkårene - Hvordan store endringer gjør du for kundene dine?**
Coverage of cyber		Hovedpilarene, 1. party loss - event management loss, og 3. party loss - de søylene er relativt like, men så er det variasjoner innenfor der. . Hvis du ønsker å dekke det du er eksponert, man får ikke noe rabatt for ikke å ta med deler man ikke eksponert for. Det er det man er eksponert for som koster, så det å ta med deler man ikke eksponert for koster tilnærmet ingenting ekstra så hvorfor ikke ta det med. Så derfor er det sånn at tankegangen med pick and choose er bra, men det blir veldig sjeldent brukt. **Tidligere vilkår - har du tilgang til disse?** - Tilgang til Gamle AIG and Zurich vilkår - De norske vilkårene ser man godt forskjellig mellom de internasjonale og norske 54:11 **Lese vilkår** Når dere leser vilkår er det et par ting som er viktige å se på - Hva er triggeren, hva trigger forsikringen. Det må man alltid lete etter, det kan være forskjellige triggere under ulike elementer. På ansvarsforsikringen er det stort sett krav fra myndigheter, mens på avbrudds delen eller håndtering av hendelsen vil det være det at man

		har oppdaget. Noen skriver at det står occurred in the insurance period. Det vil si at hendelsen har skjedd. Det vi stort sett alltid ber om å få er "discovered" for hvilken tid skjedde det. Hvilken tid ble maskinen infisert. Det er vanskelig å stadfeste. Så ser vi også om det er noe retroaktiv dato. Noen sier at vi tar discovered, men at vi har retroaktiv dato tilbake til kanskje 1 år eller noe slikt eller fra etablering av forsikringen. Da kan man også ha en problemstilling. Derfor skal man se etter triggerne, hva er det og begrensningene innenfor triggerne og unntakene er også viktig å lese. De gamle zurich vilkårene og egt. de nye også er veldig på å skrive hoveddekningen opp og så skriver unntakene og under unntakene kan man få dekningen, en såkalt carve-back **Hva er en carve back** At man har et unntak, for eksempel på ansvarsforsikring unntar vi kontraktsansvar. Det er et rent unntak, men så sier vi at vi har en carve-back for kontraktsansvar som man ville hatt dersom kontrakten ikke ville vært tilstede. Rent rettslig erstatningsansvar. Så dersom kontrakten omhandler det, er det ikke unntak hvis jussen sier at det skulle vært sånn allikevel. Det kan være en carve-back. Man kan ha unntak for visse typer hendelser på property, og det er en av de unntakene vi har sett har kommet på tingforsikring vi har unntak for skader som følge av en cyber hendelsen, men vi tar inn igjen hvis det fører til brann/vannlekkasje etc. vi har et unntak, men så sier vi at du får litt allikevel. Zurich har gjort dette flere ganger. De dekker ikke fines and penalties, og så står det på unntaket, så står det bakerst om det ikke er lovlig tillatt. Mens på andre står det at de dekker det om det er lovlig. Dette gjør at man får dårlig oppbygging av vilkår. Det kan dere se selv. Og så er det litt sånn man jobber med definisjoner. Noen skriver lite, mens masse definisjoner. Andre skriver mye, men lite definisjoner. Mye av det samme går igjen med små unntak. 58:03 **Når forsikringsselskaper lager definisjoner, baserer de på ?**

		Det er mye copy-paste, de skjeler til hverandre. Man prøver ofte å bygge opp vilkår, basert på vilkår tradisjoner i selskapet. Men så skjeler man veldig til hva andre gjør. Det er vel noe av grunnen til at de norske vilkårene er litt dårlige siden de skjeler til andre norske selskaper/vilkår. Vi har veldig få gode norske cyber vilkår. Trygg sitt er et av de bedre. Men det kunne fortsatt vært bedre. **Hvis vilkårene konvergerer, Hvordan bygger man opp et konkurransefortrinn da?** Kan være en blanding, for SMB-markedet er det ofte det at man ønsker å samle forsikringene et sted. Man ønsker ikke å ha mange selskaper å forholde seg til. Dette kan være lojalitet faktoren. Så er det også litt prising forskjell. For de store virksomhetene, selv om dekningen kan være litt ulik. Vi vurderer jo små ulikheter, men så er det også hva slags panel er det de tilbyr. Hvem er det som er støtteapparat som de tilbyr bak. Så kan det være erfaring med forsikringsselskap, skade erfaring. Sitter på et anbud for en kunde der hvor vi har 2 veldig gode tilbud innen. Der jeg personlig ville valgt det ene, og kunde sier nei vi har dårlig erfaring med de, så vi vil ikke ha de. Jeg synes vilkårene er mye bedre og bedre oppsett. Prismessig er de nokså like, de får noen ekstra dekning på det vilkåret som de ikke får det på det andre, alt i alt synes jeg det ene er bedre. Men jeg ser kundens reservasjon, de har noe dårlige erfaringer med skadeoppgjør så de ønsker ikke å bruke det. Så det er in-the-end. Det man kjøper er skadeoppgjør. Sant skal sies så har de erfaring på et helt annet produkt, så jeg mener det ikke er overførbart. Vi har også i andre tilfeller, der vi har fått inn gode tilbud med lavere premium og nokså like vilkår, men vi har sagt at vi ikke kan anbefale dette siden vi vet at dersom man kjøper dette vil man få problemer når man har skade. Vi ser at man bruker mye tid og ressurser for å få igjennom skade. Derfor er det slik at med meglere kan man dra på hele erfaringsbanken deres. **Tar dere som forsikringsmeglere hensyn til den potensielle risikoen at et forsikringsselskap kan gå over ende dersom de er overeksponert ved en hendelse?**

	Influence of changing market conditions	Som med AIG som var veldige dominante i markedet, ikke så mye at de ville gå under for vi vet at de blir reddet. Det har vi jo sett før. Men det er jo noe av grunnen at finansmyndighetene har kommet med krav om å unngå silent cover. Da har man jo tatt på seg en større risiko enn man har tatt en premium for. Det er jo det med en ubalanse i markedet, med noen få dominante aktører, mister man fort små aktører. Da kan de store dreie markedet i en annen retning enn hva man ønsker. Nå er det i de nordiske markedet er finansmyndighetene såpass strenge, spesielt med avsetning og slikt. Det man kan være redde for er at selskapene skal trekke seg ut. At de velger å slutte og tegne cyber. Det ville være ugunstig. Da ville hele markedet rakne. Når noen begynner å redusere kapasiteten, begynner andre å tenke. Man ser jo derfor ringvirkninger i markedet. Det er viktig at man har stabile, gode aktører som klarer å tenke langsiktig. Det er noen grunn at man kommer inn som en helt ny aktør. Spesielt på SMB markedet, tegner man forsikring for et selskap. På de virkelige store er det mange aktører som tegner. Der hvor de nye aktørene går inn på toppen for å lære. (Under layered insurance) Gått mer over til layered insurance relativt til coinsurance siden man har sett at det er lettere bytte ut et lag enn å begynne å restrukurere coinsurance-avtalen. Det vi ser i markedet er at noen har veldig appetitt for å være langt nede der hvor det er et større premium-volum. Mens andre vil være mer på toppen. 1:04:11 **Det nederste layered tar første-støyten?** --- Prater om denne layered for å se hvem som tar støyten med henvisning til illustrasjonen på tavlen --- Kapasitet Premiumen - koster cirka like mye uansett hvor man er hen. Når man sitter og beregner hvor stor man tror skaden skal bli, hvis man regner med at det først skjer en skade så går hele tårnet uansett. Da er premiumen lik uansett siden da brenner man alt. Men hvis man ser det at med 80% sannsynligheten ligger innenfor et visst området

Coverages is trending upwards		så vil premiumen være betraktelig større for de som kan bli trukket. En trend vi ser i cyberforsikring er at man kjøper en liten forsikringssum i forhold til behovet. For man har egentlig ikke skjønt hvordan eksponering kunne ramme, sånn at hvis du ser på statistikken for hvor mye av forsikring som har dekket de ulike elementene så ser man nesten alt 80-90% går til å håndtere hendelsen, så er det nesten ingenting igjen til ansvar eller avbruddsforsikring. Det er fordi man har kjøpt en for liten sum. Det man ser generelt i markedet er at summene øker betraktelig. Tidligere så man kanskje et par hundre millioner. Når er man fort opp en mrd. 1:06:40 **Har du noe data på dette som vi kunne se på?** Vi har noen rapporter som er kanskje litt gamle. Rapport fra USA ... etc. **Kristoffer prater kløynete om et tak på kapasiteten** Forsikringen har blitt så bred, men har ikke kommet helt dit på cyber. **At dekningen har blitt for bred og man må begynne å redusere kapasitet for ikke å overeksponere forsikringssektoren mot et omfattende angrep.** Foreløpig er det ikke noe som det har kommet noe offisielt på, men det har vært noen diskusjoner. I utgangspunktet at de har vært komfortable med det, det diskuteres stadig vekk om det kommer til å komme innskrenkninger. Men foreløpig er produktet så nytt at man heller ser på å justere premiumen. Sånn man har bygd opp forsikring med de 3 hovedtårnene. Men så har man i tillegg utpressing delen, hvis utbetalingene bare gikk på utpressing kostnader kunne det være at på sikt sier man at man dekker håndtering, men vi dekker ikke utpressing kostnadene. Men vi ser at det har ikke vært utviklingen. Det er fordi vi ser at de fleste selskapene ikke vil ha utpressings forsikringen siden man ikke får igjen dataene sine. Det oppleves bare som en oppmuntring til en kriminell organisasjon. Vi har en utvidelse på beterments dette er stort sett unntatt på de fleste forsikringer, man får erstatta tilbake til den

		tilstanden man er i. Men for cyber har man fått en liten utvidelse på betterments for å kunne forbedre systemet nok for at det samme ikke skal kunne gjenta seg. Hvis det var hovedboken av dekningen så klart ville det kan være noe som virka, på sikt kunne si at nei dette her, nå driver jo vi å forbedre/oppgraderer systemet til virksomheten. Det er ikke intensjonen for forsikringen, men fremdeles det er ikke det som er den store kostnads bøylen. Det som vi har sett på de skadene som har vært, det som er i kjernen av det som er ment å dekke. Så lenge det er det som rammes i hovedsak. Så tror jeg ikke vi kommer til å se de store begrensningene, men hvis du begynner å få masse krav som er litt odds and ends, da tror jeg man vil kunne se det. Men ikke foreløpig **Ang. den utpressingssakene, de forsikringspolisene man holder er helt konfidensielle, så om man har forsikring på dette vil det være et signalement til markedet** Vi har en annen type forsikring som heter Kidnapp and ransom forsikring som vi tegner for en del kunder. Det har vært en veldig typisk forsikring for ansatte som reiser til urolige områder. Da får man dekke en spesialist konsulent gjerne med militær bakgrunn som kommer inn og forhandler med kidnappere og dette kan man få dekka. Slike typer poliser har konfidensielle klausur, hvorhen det blir allmennkunnskap så slutter denne å gjelde. På cyberforsikring er det som regel en konfidensiell klausul under hvis man kjøper extortion. Men den er ikke så strict som det K&R klausulen er. Det er en begrunnelse er det kjent at man har en forsikring kan den utnyttes, og det gjelder egentlig alle mulig forsikring der hvor 3. parts forsikring kan være dekket. Til kunder sier vi at ikke fortell kontraktspart hvor stor forsikringssum du har, for hvis det skjer noe vil de kreve så mye som mulig. Så man skal ikke eksponere den mer enn mulig. Man skal forsøke å begrense din egen eksponering. Man kjøper en sum som er tilstrekkelig, men ikke nødvendig å gå rundt og vift med det. Det samme gjelder med cyber, de fleste har dekket å håndtere en utpressing, men det å dekke selve ransomen den er ikke alltid dekket, ofte er dette en utvidelse du må kjøpe. Men det vi ser at den blir veldig lite

Coverage of Cyber		benyttet. Virksomheten vil heller ikke bli oppfattet som en virksomhet som betaler, man ønsker ikke det ryktet på seg at de er en som betaler. Derfor er konfidensiell klausul på cyber vært noe mildere enn K&R. 1:13:28 Man kjøper ikke forsikring for å unngå og gjøre ting. Det er når man feiler at forsikringen skal slå inn. Det skal være en katastrofesikring. Men hva defineres som en katastrofe for en bedrift er betraktelig forskjellige mellom små og store aktører. Det er for å beskytte bunnlinja di for ikke å få de store påvirkningene når det oppstår store ting. Det vil du se i egenhandel strukturen, på vanlig tingforsikring har man en egenhandel som er monetær på ting og så har man en waiting period (avbruddstid)/karenstid på avbrudd litt samme på cyber. Men på cyber har man bygget opp i noen tilfeller, noe man kan se på allianz sine vilkår, de tar en monetær sum og så har de 12 timer på avbrudd, men når de 12 timene har gått så dropper de ned og tar alt. Det gjør man ikke vanligvis på tingforsikring. Hvis man har 48 timer karens, så har man 48 timer, da dekkes ikke tapet ditt. De første 48 timene. Og det burde man også se på mange av de andre vilkårene. De dekker ikke de første 8-12-24 timene, det er det tapet man må bære selv. Man får bistå, men inntektstapet de første timene vil man ikke dekke. Grunnen til dette er at forsikringsselskapene ikke skal plukke opp alt småting, daglige ting. For dette skal man ha kontroll på selv.

Appendix A3 - Transcription and Analysis of Interview with Glennie Ingebrigtsen 13.02.20

Semantic Codes	Latent Codes	Transcription of Interview
		Glennie [00:00:00]: Så ønsker jeg at hvis dere skal bruke noe av det i oppgaven, at jeg leser gjennom før dere leverer. Kris [00:00:08]: Altså hvis det skulle være noe konfidensielt, er det mulig å skrive at man ikke skal publiseres. Glennie [00:00:17]: Jeg er bare litt nysgjerrig hvordan eller hva fikk dere til å tenke at cf har dere lyst til å skrive om. Kris [00:00:27]: Ja det var helt tilfeldig, jeg var i en middag i regi av Bi og ble kontaktet med noen fra finans Norge, og helt tilfeldig begynte å prate om cyber eksponeringen vi har nå, og hvordan forsikringsselskapene skal tolke det, så nevnte hun Maersk, og da innså jeg hvor omfattende angrepene kan bli, også begynte vi å se på hvordan man kan mitigate risken, og mulige måter å takle dette på. Og da kom vi innpå forsikring, jeg vet ikke om det er noen skoler som tilbyr forsikrings linjer som ikke er etterutdanning. Glennie [00:01:12]: Ja, er det noen skoler som har det? Kris [00:01:14]: Jeg vet ikke, jeg vet bare om St.Gallen har en egen insurance department, men jeg vet ikke om de tilbyr noe for studenter i det hele tatt. Mats [00:01:22]: Ja, for han veilederen vår driver å utdanner i Norge, men det er vel bare etterutdanning. Glennie [00:01:27]: Ja, for det vet jeg, det er en del av. For vi har jo operasjoner og anlegg i Brasil, og der har de egne forsikrings linjer, for studenter. Men det er ikke kjent for oss her. Kris [00:01:44]: Synd det, for det er utrolig spennende. De burde hatt det i kombinasjon, for det er jo så omfattende, altså når vi startet så ante vi ikke. Vi tenkte bare at forsikringsselskapene stod bak alt, også plutselig så er det ledd med meglerne, også et ledd med reassuranse. også finner vi ut nye ting med captives, det er jo alltid noe nytt å dykke inn i. Glennie [00:02:06]: Ja men så fint, da har dere på en måte fått på plass de ulike aktørene.

		[00:02:18] Kris: jeg vet ikke om du kanskje har lyst til å fortelle litt om deg selv først jeg? ... Glennie ferdig med å snakke om seg selv på [00:05:56]. [00:05:58] Kris: Så du er primært øverste leder over captive? [00:05:58] Glennie: Administrativt så er jeg det, men captivet er et eget AS, så formelt og driftsmessig så rapporterer det opp til styret til industriforsikring. Men når jeg sitter som leder for hydro sin forsikringsavdeling, så må jeg jo ha veldig god innsikt og kontroll på captive for å hele tiden vurdere; hvordan kan vi best bruke captive til fordel for hydro, en ting og avbruddsforsikring, lønner det seg her å bruke captive eller ikke, eller skal vi bare bruke det kommersielle eksterne markedet? Så sånt sett så er captiven en integrert del på en måte, at vi hele tiden må samarbeide for finne ut hvordan vi best kan optimalisere captivet,
	Influence of regulations	men captive er underlagt egne lover og regler, og har fått konsesjon av finanstilsynet som de må forholde seg til. Og all rapportering som følger. [00:06:53] Kris: Så du har en egen driftsavdeling i captivet, eller er kun et skall? [00:06:58] Glennie: Nei, dere kan også vite at hydro har verdens eldste eksisterende captive, det ble etablert i 1920, så vi har jo jubileum i år. og captivet er baser her i norge, mange andre har captive som de har i Luxemburg, i Sveits, Bermuda, litt mer sånn skatte optimaliserende hendelser, mens her er vi i Norge og vi betaler vår skatt, og vi opererer, det er jo et mini forsikringsselskap, til forskjell fra en del andre
Role of captive		captives, så operer industriforsikring som det du kaller et direkte tegnende captive, det vil si at det er vi som står i front, vi gjør vår egen underwriting, altså vi prissetter, vi gjør skadebehandling. Også kjøper vi selvfølgelig reassuranse. Men det at vi har et front office, et reelt captive i den forstand at vi har vårt eget forsikringssystem, utsteder poliser, får premie, gjør skadebehandling, setter av reserver, henter inn fra reassurandørene. Så ja det er ikke et skall, det er et reelt
	Influence of regulations	captive, og det er jo i forhold til internprising og EU regelverk, er det jo mer og mer at captivene må dokumentere at de er et reelt captive. At de faktisk må

		dokumentere hvordan de (captivene) gjør prisingen, tidligere kunne man bare få et eksternt selskap til å prise for seg, så fulgte captive bare den prisen, det står seg nok ikke lengre nå. Nå må du selv dokumentere at du gjør en aktuell beregning, at du klarer å vurdere risikoen din selv, og det er viktig. Og det kan vi gjøre, vi kan vise at vi har en filosofert måte å beregne risikoen på. Så i dag så er det fem personer som er dedikert til captive, også kjøper captive inn tjenester fra rådgivere i hydro sin forsikrings avdeling.
Outsourcing functions		[00:09:14] Kris. Ok, hvilke deler av captive outsourcer dere, eller er det noen deler dere kan outsource? [00:09:18] Glennie: Det vi har outsourced da, er risk og compliance funksjonen, og det gjør vi i samarbeid sammen med andre Norske captives også. Det er litt vanskelig at den som jobber i captive også skal sitte å kontrollere seg selv, så derfor er den satt ut. Også er intern kontroll biten satt ut. [00:09:48] Kris: Altså slik jeg antok, så er det slik at industriforsikring tar all forsikringen for Hydro, men har dere ekstern, der hvor Hydro ikke går gjennom industriforsikring? [00:10:00] Glennie: Det hender. Det som er med industriforsikring er at de tilbyr nesten all forsikring som Hydro har behov for, de forsikrer ikke directors and officers, styreansvarsforsikring da, der må vi ha en armlengdes avstand, så der tar captive ikke noe risk.
Role of captive		Captive kan operere som et direkte tegnede captive, hvor det er de som utsteder polisen og har et kontraktsforhold direkt med hydro eller så kan det opptre som et reassuranse captive, som nok er mest vanlig. Det vil si at de står bak et kommersielt selskap, og at det er AIG, Zurich eller hvem som helst som har det direkte kontraktsforholdet med Hydro, og det er den gangen vi har beveget oss på en del av produktene, ikke på ting og avbrudds forsikringen, som er den største forsikringen som Hydro har, der fronter captive direkte, og det er også fordi her mener vi at vi har veldig god kompetanse, som vi har bygget opp gjennom mange år. og vi har også egen ingeniører som er med å gjør survey
	Influence of experience	på fabrikkene, så der føler vi oss veldig kompetente til å stå i front, vurdere premien, kjøpe reassuranse. Så der operere vi som en direkte tegnende. På ansvarsforsikring, på underslagsforsikring, eller miljø

		ansvarsforsikring så opererer vi som et reassuranse captive. [00:11:41] Mats: Gjelder det cyber også, eller hva gjøre dere der?
	Lack of information	[00:11:46] Glennie: Der er vi med å ta litt risk, men der også er vi ikke direkte nei. [00:11:53] Mats: Og det har med at dere ikke føler at der ikke har nok kompetanse, eller? [00:11:57] Glennie: Der gjorde vi, da den ble tegnet, det var en forsikring som vi tegnet i 2018, og da gjorde vi en vurdering på hvordan og om, først om i det hele tatt captive skulle være involvert, og hvordan skulle captive være involvert i det. Også er jo det et forsikringsoppgjør som pågår nå og som også ble omtalt i mediene, vi er jo et børsnotert selskap, så jeg tror ikke jeg vil gi noe mer informasjon nå om akkurat nå. Men at vi tar noe risk der, det gjør vi jo. [00:12:29] Mats: Men var det en spesiell grunn til at det skjedde i 2018 eller, var det bare da det var naturlig, hvorfor ikke før? [00:12:35] Glennie: Både ja og nei, dette kommer litt ann på hvordan forsikrings avdelingen jobber, de jobber tett med ERM organisasjon og hvordan Hydro
	New treats	også jobber med ERM, og det er at det var noen år siden da at cyber risk kom opp på risiko kartet til Hydro, og vår oppgave er jo å at vi må jobbe utadrettet og utadrettet, og sørge for at vi forstår til en hver tid hydros risk og nye risikoer, og da kunne gå ut er det et forsikringsprodukt her som kan avlaste, den risken hvis Hydro ønsker det. Så det vi gjorde når det kom opp på hydros risikokart, så må jo vi snu oss ut, og for det første så må vi jo se på de forsikringen vi allerede har, hvordan dekker de forsikringen hydro allerede har den risken. også ser vi at her er det noen gaps, okei, hvordan kan vi dekke disse hullene, er det mulig og til hvilken
	Emerging market	pris. Og da måtte vi ut å sjekke markedet, og når vi begynte å gjøre det i 2016, så var det ikke mange, det var jo noen cyber produkter der, men det er jo produkter som er mer rettet mot finansielle institusjoner, banker og den type ting. Da var jo frykten med cyber security, altså IT sikkerhet, som går på det mer konvensjonelle beskyttelsen av data. Sant, bedrifts hemmeligheter, eller personopplysninger, det var jo det forsikringen da dekket, og som den var opptatt av. Og det er viktig for Hydro, men for oss så er vi jo kanskje

		en større risk er jo hva hvis vi ikke får produsert, hva hvis drifts systemene våre stopper, hva hvis raffineriet vårt ikke virker, det blir en pot freeze, det er da vi får de store tapene, da får vi store inntektstap. Og cyber produktet dekker jo ikke det. Så vi måtte hele tiden kartlegge hva som er viktig og hvordan skal man kvantifisere de tapene man har, hvordan kan man ha et tap uten, eller hvilke forretningsområder er mer utsatt for det tapet som denne cyber dekningen kan gjøre, og hvordan kan vi prøve å sikre opp det cyber produktet ikke dekker opp, og utvide de eksisterende forsikringene vi har. Så vi hadde jo da en anbudsprosess på cyber som Willis hjalp oss med, Willis var da megler på en del produkter som allerede hadde cyber elementer i seg, så det var naturlig å bruke Willis til å dekke de hullene i de forsikringene som de var megler for. Så vi prøvde jo å utvide det vi hadde, samtidig som vi sjekket hva vi kunne få på en cyber dekning, og da brukte vi over ett år, på å forhandle det, finne ut hvilken aktør som vi syntes passet best for Hydro, skreddersyr litt disse vilkårene. Og da har vi jo gått ut i media, at den som er lead på forsikringsproduktene når det gjelder cyber er AEG.
	Structure of policy	Men cyber er som alle de andre produktene vi har, de bygges jo opp som et tårn, med ulike lag, fordi vi kjøper så mye kapasitet, at det ikke er et selskap som kan tilby så mye. Men da brukte vi AEG som lead, også fikk vi med oss alle de andre forsikringsselskapene på de terms og conditions som AEG kom med. så da fikk vi den på plass fra 01.01.2018. Men da startet vi prosessen våren 2016 også var det på plass i 2018. [00:16:48] Kris: Kan det ha vært Maersk angrepet som utløste det? [00:16:51] Glennie: Nei. Altså det er klart at alle hendelser rundt omkring i verden er jo med på å sette risikoen, eller skape en slags bevisstgjøring i organisasjonen på risikoen, det er jo klart. Men at det var DEN som gjorde at vi tegnet den cf, man gjør jo en egen analyse av risikoen i sitt eget selskap, også blir man jo egentlig minnet på når det skjer hendelser. Men det valget om å tegne cf var en avgjørelse på CFO nivå. Og som var forankret i de ulike forretningsområdene om at dette var en forsikring man ønsket å tegne. Også
	Emerging market	tenker jeg også at vi så en window of opportunity, ved at vi var relativt tidlig ute, og selv da i 2016-17 så hadde

		det ikke tatt helt av med skader, slik at vi så at den prisen vi fikk var under markedspris, så det er noe med å benytte et slikt vindu. [00:18:12] Mats: Ja, for vi har jo fått inntrykk av at de ikke tør å ta like mye risk lengre forsikringsselskapene som det de gjorde tidligere.
	Lack of data	[00:18:21] Glennie: Det ser vi, at kapasiteten, selskapene tar fortsatt risk, men de gir mindre kapasitet, så nå trenger man flere selskaper for å dekke opp den samme forsikringssummen. [00:18:33] Mats: Men sånn etter angrepet på Hydro i fjor, blir det da en ny vurdering fra forsikringsselskapene eller fortsetter dere med samme polisen.
	Structure of policy	[00:18:45] Glennie: Det er en ett års polise, slik at da går vi inn i en fornyelsesprosess, og da må jo forsikringsselskapene i god tid, hvis dette er noe de ikke vil være med på, bør varsle det. Så da starter vi en fornyelsesprosess hvor vi forhandler om terms og conditions, og vi jobber med å holde prisen så lav som mulig, men det aller viktigste er å beholde den dekningen som vi synes er viktig. [00:19:11] Kris: Så premium er bare kontraktsfestet for et år.
	Emerging market Lack of experience	[00:19:16] Glennie: Men så er det jo ofte man klarer å fornye med samme terms og conditions, så det er egentlig en veldig enkel fornyelse. Men det er jo klart at cyber som er en såpass ny risk og nytt produkt. Det å tro at de skal ha akkurat samme premium og samme egenandel, ett år etter en sånn skade, og de har hatt masse erfaringer og masse skader på verdensbasis, så det er klart at det ikke ble akkurat samme terms og conditions, men vi er fornøyde. [00:19:49] Kris: Så den premiumen er kanskje konfidensiell eller? [00:19:51] Glennie: Ja, ikke før jeg har fått samtykke til det nei. Men det kan en megler gi dere litt sånn generelt. De kan jo si litt generelt om hva slag limit man kjøper. [00:20:25] Mats: Men sånn med tanke på risiko, som blir beregnet i en forsikring, sånn etter angrepet på Hydro i fjor. Blir da forsikringsselskapene mer skeptisk, siden dere ble angrepet, eller tenker de at da har dere skjønt at det er reelt.

	Demands to customers Risk potential Influence of experience Influence of experience	[00:20:43] Glennie: Dere bør jo snakke med litt flere forsikringsselskaper enn gjensidige, hvis jeg var dere ville jeg snakket med Zurich og AEG for å nevne noen. Men tilbakemeldingen vi får fra forsikringsselskapene kan være litt todelt, veldig positivt i den forstand at når en kunde har vært gjennom en skade, så har det noen ganske kraftige lessons learned, så vi har en helt annen awearness på risikoen, og vi har bygget opp en ny infrastruktur, så det er klart at vi stiller mye mer rustet nå mot et nytt angrep, så det er jo positivt. Sånn sett så ønsker de å være med videre, også ønsker også ofte forsikringsselskapene å være med videre for å hente inn det de har tapt. Og da håper de jo, og da er det jo vår jobb å gi de trygghet med vår risk, at det ikke skal skje en ny skade nå, slik at hvis de er med videre fremover nå så kan de få hentet inn det de har tapt, det er jo det de tenker. Samtidig så har det også blitt demonstrert at vi er en target, er det tilfeldig at vi ble angrepet, og slik som angrepet skjedde, så viser det seg at dette ikke var tilfeldig, så de tenker kanskje også at, ja de er bedre rustet, men samtidig så har det blitt demonstrert at det er noen som ønsker å prøve seg på de. Det kan du kanskje si om flere store selskaper, at de er noen man ønsker å prøve seg på. Så det har vært litt delt, men min erfaring er vel at de nå tenker at selskapet nå er en bedre risk, enn et selskap som ikke har vært utsatt for et angrep og som ikke har hatt en skade. Vi snakker... [00:23:28] Glennie: Også er det når vi velger aktører, vår forskningsstrategi er langsiktig partnerskap. For dette er en ganske kompleks risk på alle mulig måter. og vi ønsker å ha forsikringsselskaper som forstår risikoen, slik at hvis det skulle komme en skade, så er det ingen som skal komme; "hæ det trodde vi aldri kunne skje". De skal vite hva de tegner, og de skal gjøre en ordentlig underwriting. Vi søker ikke i utgangspunktet et opportunistisk marked, aktører som bare er inne et år og trekker seg ut. Vi ønsker å se en langsiktighet, som også gir en forutsigbar prising. Slik at når du gå inn på et program hos Hydro så er vi ganske klare i forventningen om at du er med oss og da er du også med oss når vi har en skade. men vi har alle en felles interesse å bedre sikkerheten, for det koster

		innmari mye for oss også. Det er ikke slik at vi har forsikring så da blåser vi i det. Målet er jo at det skal være partnerskap, at vi sammen skal jobbe, og vi har en felles interesse av best mulig risk. Så da skal de også være med oss neste år også. [00:24:47] Kris: Da kommer vi kanskje inn på selve angrepet, men hva slags krav stiller dere til quick response tid, som er innarbeidet i polisene. [00:25:02] Glennie: Og det er en sånne ting har en del hvordan synes jeg det funket osv. når vi er ferdig med skaden, er det mye lettere å snakke om denne skaden, og hvordan ting funket, etter. Så det kan jeg ikke kommentere. Men man kan jo si er at det vi har snakket med forsikringsselskapet om er at når denne skaden er ferdig så skal vi sette oss ned å ha en lesson learned, for det er klart at ting som de kanskje lover som ikke fungerte helt, og så tror jeg at de kan lære litt av våres tilbakemeldinger, også kan vi lære litt om hvordan vi håndterte dette her. For dette her er en unik sak, ved at det er så mange fabrikker som ble berørt, vi hadde over 100 fabrikker som ble berørt. Vanligvis har vi en skade på en fabrikk, så kan alle konsentrere seg på den ene fabrikken og det ene tapet. Her kan du tenke deg du skal dokumentere opp et tap, og forsikringsselskapene skal også motta (dokumentasjon). Et tap da som følge av en konsekvens som har inntruffet på over 100 fabrikker, så det er ingen som har erfaring med det, derfor blir det veldig nyttig læring for både dem og oss, som vi tenker vi kan gi tilbake til selve forsikringsbransjen. At man kan forbedre produktet, og forbedre hvordan man takler og håndterer et sånt skadeoppgjør. [00:26:29] Kris: Hvor lang tid antar dette at dette oppgjøret vil ta? [00:26:35] Glennie: Nå denne identity perioden vil jo være litt førende for det spørsmålet. Vi har en identity periode som ikke er over enda, og da er det naturlig at vi i hvert fall venter til den er over. Også har det noe med det jeg kanskje ikke var så bevisst på her, at man kommer litt senere i gang med å dokumentere opp tapet, i hvert fall når det gjelder avbrudds delen, for systemene var jo nede. Så det å begynne å hente tall, fra et system, historiske tall som du trenger for å dokumentere tapet ditt. Du har ikke tilgang til det, så du må vente til systemene er oppe å går igjen, så man kommer litt sent i gang. Dette er jo ikke noe som tar et
	Professional support	
	Damage potential	
	Lack of experienc	
	Lack of data	
	Risk potential	

		år, det tar lengre. Men vi håper at vi skal være ferdig i løpet av året, hvis det er noe igjen, hvis det blir noe rettssak, eller ...., så kan jo det drøye. Men det er ingen indikasjoner foreløpig, Vi har en veldig god dialog med forsikringsselskapene. [00:27:51] Mats: Men sånn krav, forsikringsselskapene stiller jo ofte visse krav til sikkerhet, og visse ting som må være på plass, har det vært noen endring i det. Fremover må dere bli bedre på det og det? [00:28:16] Glennie: Har ikke fått noe sikkerhetsforskrifter eller noe krav om det, men det er klart at når vi fornyer forsikringen så kommer selskapene med et questionnaire, og det har vi fylt ut. [00:28:26] Mats: Så det er egentlig ikke noe mer enn det? [00:28:28] Glennie: Nei. [00:28:31] Kris: Har dere fått noen andre forespørsler fra selskaper som kanskje vurdere eller ønsker å tegne cf. [00:28:44] Glennie: Da vi tegnet den, så var det mange andre i captive gruppen og i Norima, Norima er en nordisk organisasjon for risk. Og det er en gruppe som møtes noen ganger i året, diskuterer og tar opp ulike ting knyttet til veldig mye til forsikring. Vi har jo holdt foredrag i forkant av angrepet om prosessen vi hadde med å inngå forsikringen, og hvorfor vi inngikk den. Så det har vært veldig stor interesse for det fra andre selskaper, som vi har fått en god del henvendelser fra, flere henvendelser på det. Også er jo selvfølgelig alle nysgjerrige på hvordan forsikringen faktisk virker. Og nå gikk det jo frem av kvartals rapporteringen forrige uke, at vi har fått utbetalt så langt 220 millioner NOK. Så da ser man jo at forsikringen responderer, også uttaler vi jo også at vi jobber videre med saken, og at når man er sikker på at man får mer, så kommuniserer vi det også. Så ja det er stor interesse og mange spørsmål. Kris snakker om intervjuet med Nanna Unhammer. [00:30:37] Mats: Men risikovurdering når det er dere som captive som er mye med i prosessen, hvordan arbeider dere, for det er jo en veldig vanskelig risiko. [00:30:54] Glennie: I forsikrings avdelingen så er jo vår oppgave å hele tiden forstå risikoen, og kunne

Demands to customers

Lack of data

		tilrettelegge og kunne tilby relevante forsikringsprodukter. Og kunne kommunisere i forhold til den risikoen som er beskrevet, hva er dekket og hva er ikke dekket. det er ikke alltid like lett, det er ofte små detaljer som avgjør om du er innenfor eller utenfor. Du kan ha en risiko som er beskrevet som en hendelse, men så er det mange enkeltelementer som avgjøre om det er innenfor eller utenfor dekning. Det er det å kunne ha den dialogen med den som eier risikoen slik at de forstår det. Det er ikke vår oppgave som forsikringsavdeling å kartlegge risikoen i Hydro, men vi skal samarbeide og bistå de som eier risikoen. Og i Hydro så har vi en enterprise risk management organisasjon som jobber top down, med risk og som fasiliterer kartlegger risikoen i Hydro, som de kan løfte opp til KL og en til styre. Og da har jo vært enkelt, det er fem forskjellige forretningsområder i hydro, og hvert har jo et ansvar for den risikoen som de har. Så de skal jo rapportere da opp til ERM organisasjonen som da rapporterer opp videre, men for at de skal kunne gjøre det, så må de ha en bottom-up prosess og. Så dette er jo en top-down og en bottom-up prosess. Og når det gjelder fysisk risiko den er vi komfortable med, så der kan vi bistå i business continuity planen, workshop ikke sant være med å identifisere hendelser som kan medføre til et avbrudd, og spille inn det fra bunnen og opp i systemet. også får man etterhvert hva som er top 10 operasjonelle risikoer. Men det er bare en risiko, du har jo miljørisiko, du har social responsibility risiko, du har mange risikoer som skal rapporteres, og til slutt skal det bli hva som er Hydro's top 10 risikoer. Så vi må jo jobbe tett på hvert enkelt business area for å forstå risikoen der. også må vi se det holistiske helhetsbildet også, det er vår måte å jobbe tett å risk i hvert enkelt BA og ... for å forstå. Også må man jo vurdere hvor sannsynlig er risikoen, hva er konsekvensen, hvilke mitigerende tiltak er det vi har på plass, er vi fornøyd med den gjenværende risikoen. Nei, da må vi ha noen fler mitigerende tiltak, og hvor ender vi da. Til slutt står vi igjen med en risk, hva ønsker vi å gjøre med den, ønsker vi å forsikre den? eller ønsker vi ikke å forsikre den.
Role of insurance		For forsikring skal jo ikke være et eget verktøy i seg selv, det må jo være når du har gjort alle andre tiltak. Så blir forsikring som belte og bukseseler, kanskje man ikke har helt oversikt over risikoen, det

	Customers sensitivity to price Risk potential Influence of Changing market conditions Influence of Changing market conditions	kan jo være noe vi ikke har tenkt på som kan skje, og den konsekvensen er så stor, residual risk er så stor, så den ønsker vi å forsikre, selv om vi har gjort alt det vi kan. Hvis det skal skje så er konsekvensen så innmari høy, de vurderingene der må jo vi være inni, også kan vi gi en anbefaling ut fra, ikke sant, hva er vanlig å tegne er jo en ting, men det kan også være i forhold til pris, ok du er kanskje komfortable, men det koster så lite å forsikre det så da tar man å forsikrer det, eller ok dette koster litt, men risikoen er så stor. Så det blir slike vurderinger hele tiden som vi må sparre med den som skal betale og eier risikoen. Så vi legger selvfølgelig mye føringer, men det er jo ikke vi som eier risikoen. [00:35:27] Mats: Med prissetting, har dere et budsjett, eller er det mer basert på at hvis det er risiko så betaler dere forsikring. [00:35:38] Glennie: Vi kommer inn med hva vi tror, alle må jo levere et budsjett, og forsikring er jo en budsjettpost. Så da gir vi et innspill i budsjettprosessen om hva vi tror det kommer til å koste, også blir det, budsjettprosessen er jo tidlig så det er altfor tidlig for oss til å gi et veldig godt svar. Så det treffer jo aldri 100 prosent, men vi kan gi en range. også er det jo ikke sånt at det dukker opp nye risikoer hvert år. Slik at det plutselig kommer en forsikring vi ikke forutså eller en kostnad vi ikke forutså, det er jo de samme forsikringen sånn stort sett som fornyes, men hvis vi ser at her er den en vesentlig endring i risikobildet, eller det er en del av virksomheten som har representert en stor risiko som blir solgt ut, så må jo vi spille inn; skal vi fortsette å kjøpe den forsikringen, eller skal vi slutte å kjøpe den forsikringen. Og da må jo vi adressere det opp til det nivået hvor det hører hjemme. Hvis ikke så er det normalt en fornyelse av de eksisterende forsikringene, men cyber var jo en sak, hvor det var en ny risk og det var en prosess, vi hadde en veldig grundig og langsiktig prosess, som de da også kunne budsjettere inn, det ble jo en vurdering av CFO's sitt team, det ble en beslutning som ble tatt sammen med IT og hvordan de vurderte risikoen, de som sitter på pengesekken og forsikring da. **37:20**

	Structure of policy	**Du nevnte ang. tolke at visse ord kan gi ulike utslag på hva som blir dekket, opplever dere mye tvetydighet i due diligence perioden?** Man håper at man skal avdekke dette i forkant og ikke etterkant, men opplever nok alltid noe man ikke har tenkt på. Oi, den klausulen der, var plutselig den viktig. Man ønsker og håper alltid at man har hatt en grundig prosess. Men forsikringsvilkår kan jo være utrolig komplisert og unødvendig vanskelig å lese noen ganger, å flytte komma kan gi en helt annen betydning. Så vi hadde en del runder i forkant med cyber der vi måtte justere litt på klausulen og klargjøre litt. 38:30 **Prosessen for cyberforsikring, var den mer omfattende enn andre type forsikringer.** Dette er første gangen jeg har vært involvert i å tegne opp en helt ny forsikring. Cargo-forsikring, PD, ansvar, miljø en del type produkter er produkter som har eksistert i mange mange år så det blir hele tiden å optimalisere og forbedre for vår del, eller klargjøre. Det er jo man er med på hvert år. Er det noe man burde endre på, har risikoen endret seg slik at man må endre eller er noe man skal justere på evt. ta ut. den er der, men et helt nytt produkt det er ikke så ofte som skjer. Det er ikke ofte man går ut og kjøper et helt nytt produkt, i hvert fall ikke for oss som har lange tradisjoner for forsikring som har vært ganske tidlig ut med å bruke forsikringer. Hvis man ser tilbake til når Hydro kjøpte de ulike elementene så har vi vært tidlig ute med å vurdere risikoer og om vi skal kjøpe forsikringer for å avlaste risikoen. 39:37 **Det går litt inn på hva vi har pratet om, men karenstiden i forhold til cyberforsikring og vanlig forsikring som tingforsikring, er karenstiden (waiting period) kortere eller lengre?** Man har ulike måter å definere egenhandel eller self-retention og når det gjelder ting -og avbrudd for ting og avbruddsforsikring skal komme til anvendelse må man ha en fysisk skade. Da dekker den også

	Structure of policy	konsekvenstapet/økonomisktapet som følge av dette og da kan man enten se at man har en egenandel for den fysiske skade. Hvis skade koster, bare for å ta et tall, 1 million, hvis skaden er under dette dekker man det selv. Er den over kommer forsikringen. Også kan jo egenandelen eller waiting period på avbruddstapet er at de første 10 dagene av tapet dekker man selv. Har man fortsatt ikke klart å restaurere og bygge opp det som er ødelagt utover de 10 første dagene får man det dekket. Man har også en kombinert egenandel slik at man må bære det første tapet på for eksempel 10 millioner selv om det så er en tingskade eller avbrudd skade. Det er combined deductible. Når det gjelder cyberforsikringen så er det ulike elementer som den dekker. Det den ikke dekker er fysisk skade. Det er ikke så uvanlig at man har en egenandel for event management cost og en egenandel for liabilities og en egenandel for det man kaller network interuption som er avbruddstapet. Du må definere hva event management cost, første million betaler man selv har man også pådratt seg et ansvar må man isolerer de, hvorhen første million må man betale selv, og så har man en tredje egenandel. Så man har ulike egenandeler. Og på avbrudd da, varierer det litt om man bruker, bare har et beløp rett og slett, da sier man at de første 10 millionene dekker man selv på avbruddstapet og utover det dekker de det. Andre operer med timer og dager. Den er litt mer kompleks egentlig å forstå. Og den er veldig ulikt regulert i ulike poliser. Så kan man selv velge hva man er mest komfortabel med.
	Structure of policy	
	Structure of policy	
	Structure of policy	
		Du vil ikke si hva Hydro har?
		Nei.
		42:26
		Det er mye vi gjerne skulle hatt til oppgaven
	Lack of data	Jeg kan se etterhvert om jeg kan gi dere det, men for oppgavens del det er bare ulike måter å beregne det på. Så kan jo dere og det jeg synes er interessant er hva dere syntes, hva ville dere valgt, Hva syntes dere er enklest å forstå. Hvis dere skulle beskytte deres egen bedrift. Ville dere hatt, det er litt interessant for leseren. For det interessant for oss hvis noen faktisk graver seg

		i det. Hva er det, hva er det faktisk selskapene bør velge. Bør de velge et bestemt beløp eller bør de velge timer og dager, og hvordan ser forsikringsselskapene på dette og hva er det de egentlig mener med det. Det for meg er litt uklart. **Vi har skjønt det, det finnes ingen analyse eller modelleringsverktøy til å hjelpe driften.** Utifra det jeg sier nå så kan dere tenke på hva vi har valgt, men ... **Det er godt poeng. Vi er litt uklare ennå hvordan vi skal rette oppgaven vi skulle gjerne skrevet om Hydro, men det er vanskelig å få info..** Vi er ikke ferdige med oppgjøret. Det dere kan lese dere opp til er at polisen responderer, vi har jo fått 220 mil. Da er det ikke tatt med det vi har fått fra captivet. Vi har jo gått ut med at mesteparten av avbruddstapet ligger hos Extruded Solutions, så da vet dere at den dekker avbruddstap. Det som er nå er for oss å dokumentere det tapet vi har. Det er alltid en business interruption. Det som alltid er mest utfordrende der, vi kan jo si, vi hadde en budsjettplan på så mye. Det skulle være vår net income. Nå har vi dette, vi mener cyber er grunnen til dette. Så enkelt er det ikke, det er jo andre faktorer som gjør at man ikke oppnådde dette. Man ser jo at markedet har gått ned, har du tatt med det i budsjettet ditt?
	Damage estimation	Nei, da må du trekke fra de faktorene og det er der diskusjonen. Hva skyldes nedgang i markedet og hva skyldes cyberen. Det er det som dette går på, det tar litt å klare. En annen ting er, vet du hva vi forholder oss ikke til budsjett. Dere legger veldig ambisiøse budsjetter. Å finne det, hvordan ville hydro resultat sett ut hvis det ikke hadde vært for cybern. Å lage den Baselinen er der hvor man krangler. Det som er vanskelig er å lage den baselinen. Så budsjett kan være et utgangspunkt. Så kan man justere andre faktorer som har skjedd, men de nøyer seg ikke med budsjett. Det ville ikke jeg gjort heller, men få se hvor godt dere har truffet på budsjett tidligere år. Hva er det dere tjente i fjor, hva var volumet dere solgte i fjor. Ja, dere solgte jæskli litt, er det budjsett der realistisk dere solgte jo
	Damage estimation	

Role of insurance	Damage estimation	veldige lite ifjor. Hva solgte dere året før der igjen. De graver seg tilbake, for å finne et sted å bli enige om baselinen. Hva er det egentlig ville vært om det ikke hadde vært for cyberangrepet. Det er det mellomlegget der vi skal ha dekket under forsikringen. Det er en prosess som tar tid. Så det er ikke noe hokus pokus med den cyberforsikringen, så langt. Så lenge de ser at triggeren, yes. De aksepterer at det er en hendelse som trigger polisen. Event management cost, det er at man skal sannsynliggjøre at man har benyttet konsulenter som har forsøkt å hjelpe deg, det er ikke noe hokus pokus med det. Så er det avbruddstapet, og det er ikke hokus pokus det heller. Det er en drøy prosess, men det er ikke noe så hva er det polisene ikke trekker. Man ser at den funker, og det er en prosess hvor man må dokumentere tapet. Hvis det hadde vært, kanskje litt vanskeligere i og med at man ikke, nei jeg vet ikke.. Det er ikke noe spesielt egentlig. Det er interessant og alle syntes det er spennende. Spesielt det at man har gått ut og kommunisert tapet som følge av cyber hendelsen mellom 650-750 millioner kroner. Hvor mye av det får vi under forsikringen, og så er dere sikkert veldige nysgjerrige på hvor stor forsikringssum dere har kjøpt. Har vi klart å kvantifisere tapet vårt riktig. Det skal jeg ikke uttale meg om. Men vår CFO har sagt at vi har en robust cyber forsikring som vi er fornøyd med. 47:49 Vi er komfortabel og har en robust forsikring. Det er klart at vi i forsikringsavdelingen føler et visst press, neida. Det er en god prosess. **Dere kommuniserte tydelig at dere hadde en robust forsikring. For det var 5 eller 6 dagen dere kom ut med en press release om cyberangrepet, vil dette hjelpe økonomisk, aksjepris, roe ned angrepet** Hvis dere googler hydro cyber, kommer det oppslaget på e24 samme dag. Hvor CFO sier vi er fornøyd med å tegne forsikring, så allerede samme dag. Hydro har vært veldige åpne og transparente fra dag en. Det har vært kommunikasjonsstrategien, åpne, transparente, ta kontroll på kommunikasjonen selv. Hydro kalte inn til pressekonferanse allerede kl 15, 19. mars. Da kom det

	Risk potential	spørsmål fra salen, ganske så tidlig, har dere forsikring? Det er klart for CFO å kunne si, ja vi har forsikring. Det er med på å roe, og så er det jo ulike grunner til at man ikke kan komme å si noe mer så tidlig. Hvor mye har dere kjøpt, etc. Det har også med å gjøre man vet lite om situasjon. Man har også en dekning, flere forsikringsselskaper som også dekker extortion, Ransomware. Man snakker ikke så høyt om det. Når man i så tidlig fase ikke er så sikker på hva det kan være. Vi vurderte aldri Hydro å betale ut, men av hensyn forsikringsselskapene å gå ut å si hvor mye det er og hvor ødeleggende det er/kan være. Det ønsker vi ikke å kommunisere ut at Hydro har forsikring som dekker ransomware. Så det er en del ting som gjør man kanskje ikke kan være åpen som man kunne lyst til å være i en slik prosess. 50:04 **Hvis du ser isolert fjerner hendelsen, hvordan ville det vært for polisen da, ville den fortsatt vært konfidensiell. Den må jo være konfidensiell med tanke på ransomware, man vil jo gjerne ikke si dette til markedet og blottgjøre seg.** Det er opptil forsikringsselskapene dersom man skal kommunisere om man eventuelt har en slik dekning. Det øker jo eksponeringen. **Da blir man jo et mål.** Det ble aldri vurdert fra Hydro å utbetale det. Også kan man jo spørre om det var noe forsikringsselskapet ønsket/presset på for å bli ferdig med saken. **Vi har fått en rapport fra soderberg og partners hvor det er flere forsikringsselskaper som har sagt seg villige til ransomware. Men da på forsikringsselskaper betingelser. Så hvis det var aktuelt med ransomware måtte det og det og det oppfylles.** Det er klart at man gjør det, hvis man ønsker å hente den forsikringen. Så er det uklokt ikke å ta med forsikringsselskapene i den dialogen og prosessen. Det

		er kanskje et mindre selskaper som vurderer å utbetale. Og hvor forsikringsselskapene også gjør en vurdering om at det kan være billigere enn å gjøre det. For de har ikke det apparat eller muskler, kanskje man ikke har noe backup løsninger. Så det er kanskje veldige mange alternativer. Mens vi som har våre backup løsninger og stolte på disse. Det vi visste var at hackerne var inne i systemet vårt. Så vi måtte bygge opp på nytt igjen uansett. Så for oss var det egentlig bare å stenge ned, isolere, bygge opp på nytt. Sakte, men sikkert erstatte de pc'ene og serverne som var krypterte og infiserte. 52:12 **Når dere tegnet forsikringen, måtte dere endre noe særs på informasjonsteknologien deres, altså infrastrukturen, fikk dere noe krav fra AIG** Nei **Dere fikk jo mest sannsynlig en questionnaire**
	Demands to customers	Det gjorde vi. Vi hadde en lang prosess. Vi hadde, sammen Willis, hadde et detaljert som vi fulgte med, som vi la med når vi gikk ut på tender. Samtidig som vi la ut veldig mye informasjon om Hydro. Så inviterer vi med på markedsmøter hvor vår CIO snakker. Vi gir markedet mulighet til å stille alle mulige spørsmål de vil. VI var veldige transparente, det ønsker vi å være. Vi gjorde våre egne risikovurderinger, vi hadde egne pilotprosjekter som gikk på vurdering på OT-sikkerhet (operational technology). La med funnene fra det. Så de var vel komfortable med det de så. Så kan det hende at forsikringsselskapene, de bruker jo mange konsulenter der og, men de må også bygge seg opp kompetanse på det produktet de også. Med årene som kommer og med alle de skadene man har hatt så blir det så kanskje enda flere krav eller. Det endrer seg, dette er et produkt som er under utvikling. 53:48 **Du forventer egentlig at det vil komme noen flere krav.**
..		

Role of insurance	Professional support	Jeg forventer kanskje at prosessen blir litt annerledes, jeg forventer at prosessmøte blir noe likere det vi ser på ting og avbrudd. **Den prosessen, hvordan ser den annerledes ut i forhold til ting og avbrudd med tanke på at de sier at den vil bli mer identisk.** Kanskje man vil bli litt mer, på den operasjonell teknologi at man ønsker å gjøre mer survey. Nå er det mye på IT som er sentralstyrt som går rundt fra plant til plant er kanskje ikke så mye for seg. Men noe har de kanskje for seg at de etterhvert forsikringsselskapene har mer ressurser på å bruke på å forstå risikoen og kanskje tilby et bredere partnerskap. Hvor det gjelder å forebygge hendelser, også som vi har opplever på ting -og avbrudd hvor de gjør survey, har mange ingeniører. Kanskje de får flere it-ingeniører. It-eksperter som kan samarbeide med IT-avdelingen der. Så er jo vi en stor organisasjon som har, vi tjente på å ha bygd opp en stor it-organisasjon selv som kan håndtere hendelsen i etterkant i forhold til selskaper som ikke har den organisasjon i huset. Så vi skal bygge opp på vår egne, ikke forsikringsselskapene. Det er ikke det jeg sier, men vi ønsker å være transparente og ha med de partnerne videre i vårt risiko arbeid og skadeforebyggende arbeid. At de er med og forståelse for det vi gjør og også klar over hvor risikoen er. Så vi ønsker at de skal pøse inn mer ekspertise, selv om det kommer til å kreve mer av oss. Selv Om det er i vår interesse og. Jo mer komfortable forsikringsselskapet er mer risiko jo bedre pris får vi. Hvis ikke de har forståelse for risikoen, ikke kjenner risikoen så må de prise inn den usikkerheten. 56:34 **Det som du sa om det at dere har såpass omfattende it-avdelingen, fikk dere hjelp av eksterne konsulenter under hendelsen?** Ja, vi har jo eksterne konsulenter inne. Det var veldig naturlig og trekke på de og bruke de. **I samarbeid med AIG eller var det disse dere allerede hadde avtale med**

		De vet jo hvem vi bruker fra questionaire. Da sier man jo hvem man har samarbeid med, og så informerte vi, det sto jo i polisen at alle skal jo forhåndsgodkjennes. Men når det brenner har man ikke tid til å vente på en som sitter på kontoret sitt og godkjenne det. Så man må jo bare gjøre det som er best for å minske omfanget av skaden så mye som mulig. Så vi fikk ikke noe problemer med det i etterkant. **Så da det er dere som sitter og bestemmer hvor mange som skal inn**
	Professional support	Det er vår risk, og det er vi som sitter og lider. Så man må jo bare gjøre det som er best, og det er man forpliktet til å gjøre. Så om de kommer inn i etterkant og sier ja vi synes den konsulenten er for dyr, og så kutter man ned litt. Men det funker ikke sånn. Så akkurat det gikk greit. Enn så lenge. **Disse konsulentene hadde dere allerede avtalt kontraktfestet pris eller henta dere inn på timebasis. Noe som tilsier at de kan kreve enda mer ettersom det var såpass akutt.** Det var veldig akutt, og noen har man jo rammeavtale med allerede, og man har en rammeavtale der og så er det jo dette en spesiell hendelse slik at man bruker call-offs til det. Så må jo procurement veldig raskt finne, og det ble jo skrevet call-offs som viser til den og den rammeavtalen og nå er det cyber hendelse. Så om Man brukte de timeprisene som var der eller om det var noen andre timepriser som ble betalt det kan jo være. Men det var jo primært timebasert ja. 58:55 Det koster så mye for en senior, og koster så mye for en junior. **Kan du si hvor lenge dere hadde teamet inne, for eksempel mærsk hadde det inne et år etterpå Når de hadde hendelsen sin i 2016**
	Risk potential	Vi er i en annen situasjon. Så våre kostnader, event management kostnader er betydelig lavere enn hva maersk har. Det viser også hva slags organisasjon vi

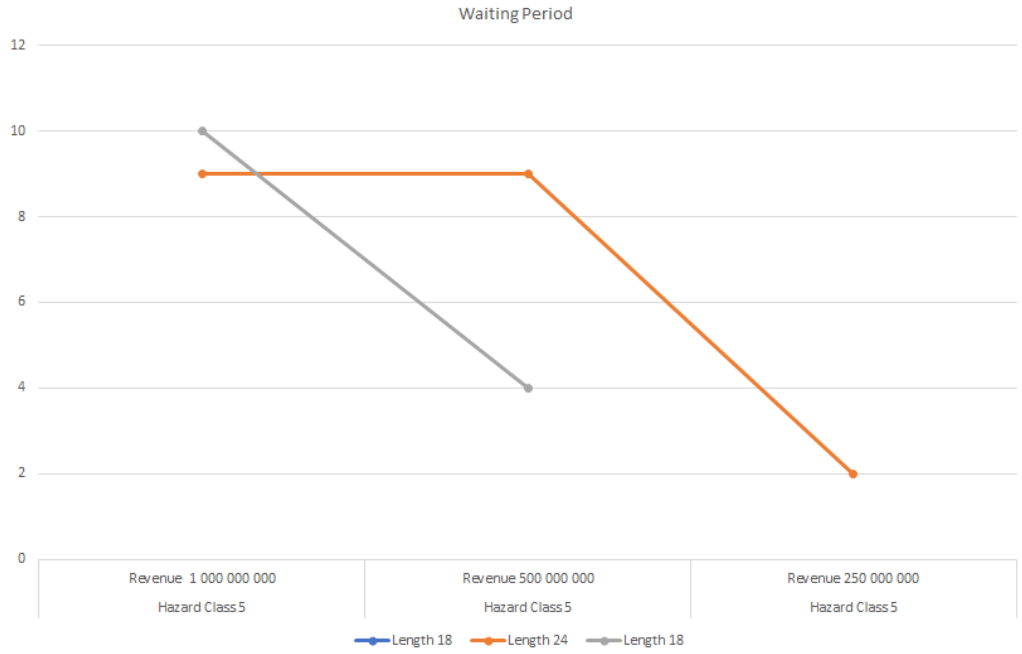
		har på plass. Også er det jo når dette skjedde, må IT raskt finne ut hvordan de skal organisere seg. Så var det 3 ulike arbeidsstrømmer. Så en arbeidsstrøm må fokusere på hvordan håndterer vi den situasjonen som er nå. En ting er nå har man besluttet å stenge nettverket for å få kontrollere situasjonen, hindre at viruset sprer seg. Legger alt død, så man finne ut hvor mye skade det har blitt gjort. Hva er det som har skjedd, hvordan har dette skjedd. Det er en arbeidsstrøm som er forensic, etter etterforskning. Så er det et team som går inn og jobber med etterforskningen så jobber de med det. Samtidig så må man jobbe med å bygge opp igjen, det er nytt nettverk. Det er ny infrastruktur. Bygge opp, som er en arbeidsstrøm, recovery. Så er det hvordan håndtere men alle de ulike utfordringer man står ovenfor nå. Vi skal betale 5000 ansatte i brasil som skal ha lønn. Bankene nekter å motta noe elektronisk fra oss, hva gjør man da. Da må man finne workarounds for det. Det koster kanskje litt også. Så man har disse underliggende arbeidsstrømmene. Noen konsulenter som etterforskning, noen som jobber med recovery og bygge opp en ny infrastruktur. Hvor lenge skal du bruke. Hvor langt tid og kostnader skal man bruke på etterforskningen. På et eller annet tidspunkt kommer man ikke lenge, klarer ikke å finne den som står bak. Så på et eller annet tidspunkt sier man nå bruker vi ikke mer penger på konsulenter for de gir oss ingenting. Vi varslet med en gang myndighetene, Kripos var inne, nasjonal sikkerhetsmyndighet var inne, datatilsynet selvfølgelig. Så Kripos er enda og gjør sin egen etterforskning så de etterforsker fortsatt. Så vi har en god dialog med de også. Så da kan man styre kostnadene ut fra den vurderingen. Så har man det å bygge opp igjen hvor man trenger konsulenter siden man ønsker å bygge opp igjen så fort som mulig. Så man organisasjon opp igjen. Vi brukte 3 mnd sånn roughly på å bygge opp igjen. Da har man noen konsulenter inne, men etterhvert kan de også fases ut siden man har en egen organisasjon som kan komme tilbake og jobbe med oppbyggingen sammen. Men så klart, man har den ekstra kostnaden. 1:02:24 **Forsikringsselskapene, har de noe grense for hvor mye konsulentarbeid de kan hente inn?**
	Risk potential	
	Professional support	
	Role of regulators	
	Professional support	

Role of insurance	Professional support	Nå har man jo forsikringssummen i seg selv som setter en begrensning til slutt. Men det er den vanlig, at det må innenfor nødvendige rammer. Og så er det jo det at i polisen så skal du, det man skal gjenoppbygge, men at vi skal nå bygge opp et helt nytt og mye bedre infrastruktur/nettverk. Det dekker det ikke. Det er standard at det ikke dekker improvements/betterments. Da blir det en prosess med dokumentasjon. Hva var det konsulentene jobbet med, bygget de opp et mye bedre system enn det vi hadde eller er det ikke det. Men hvis det ikke er noe annet alternativ enn det. Det vi hadde finnes ikke på markedet så dekker man det og. **Kan man se på det, at det hjelper både dere og forsikringsselskapet om dere bygger opp et bedre system. Hvis man ser long-term for eksempel** Det hjelper selvfølgelig forsikringsselskapet og. Men vi skal ikke droppe vedlikehold for bare å vente til det smeller så skal vi forsikringsselskapet til å bygge opp et helt nytt et. **Ang. falsk angrep, jeg vet ikke om dere har opplevd det, men hvordan forsikringsselskapet deres takler et falsk angrep og dere velger å shutdown av produksjonen, kutte systemer for å unngå videre-spredning. Siden det ikke har noe fysisk skade så på cyberforsikring dekker de også om dere velger å shut-down ved mistanke som en forhåndsregel. På tradisjonell forsikring så må det jo skje noe.** Ja, at man mistenker et angrep.
	Risk potential	**Ja, om det er i polisen eller gjeldende.** Ja, det er det helt sikkert. Jeg tror jeg husker at jeg har lest det, at vi har det. 1:06:36 **Levere 1. juli..** Det dere kan gjøre, er å ta kontakt etter 1. kvartal presentasjonen til hydro for da har det kanskje skjedd noe mer på den siden. Da kan det være noen

	Lack of data	oppdateringer da som man kan prate. Etterhvert som ting modnes hos dere, kan dere bare komme tilbake. ***Prater om kontakt med AIG/Zurich og hun skal forhøre seg med avdelingen her i Oslo og høre med dem når den relevante kompetanse er her tilbake i Oslo. Og da si i fra til oss når disse er tilbake i Oslo*** Det er interessant om dere velger å fokusere på retention om et beløp eller om dere bruker karenstid eller rundt der. For det kan varierer utifra hvilken type bedrift eller industri du er. Hvis du har kjempe konsekvenser at du er ute et par timer. Det kan for eksempel være for en bank at systemene deres er nede 2, 3,4 timer, mister man lånekunder som er inne og søker. Kommer de tilbake, Det er sikkert litt annerledes for oss om ting er borte i 2 timer. Det er ikke sikkert det er så interessant for oss, men jeg ville sett litt på det. 1:09:35 Så tror jeg at den first response er viktigere for mindre firmaer, enn for store firmaer siden vi skal ha beredskapsplan hvis det skjer noe. Hvilke kommunikasjonsbyrå bruker vi, hvilke advokatfirma bruker vi til å bistå oss. VI skal in-house ekspertise og vi skal ha en plan for hvem vi kontakter når noe skjer. Det skal vi ha på plass. Den first-response, med mindre vi velger å legge opp vår beredskapsplan på de konsulentene som forsikringsselskapet tilbyr. Det kan jo være om vi er veldig fornøyd med de. Men den er nok viktigere for mindre selskaper enn for store konserner som Hydro, Yara, Statoil. **Ja, vi har forstått at det spesielt SMB-bedrifter de er de som har behov for den eksterne hjelpen fordi de har ikke kapasiteten til å holde noe på retainer.** Forsikringsselskapene bruker også konsulenter til å beregne, forensics accountants, til å beregne og bistå tap, beregne tapet for forsikringsselskapene. Så det er mye de man skal jobbe med. Det at man har god en dialog og at de bruker gode folk er også. Jo viktigere.

10.2 Figures and Illustrations

Appendix B1 - Figure 11



10.3 Tables

Appendix C1 - Table 2

Industry	Travelers Industry 0,6 - 1,4)	Berkely (Industry 0,7-1,15)	Philadelphia Insurance (Industry 1-4)	QBE (Hazard 1-5)	CFC (Risk tier 1-5)	Travelers (Industry 0,6	Berkely (Industry 0,7-1	Philadelphia (Indi	QBE (Hazard	CFC (Risk tier	Average Hazard Class	
Associations	0.25	0.666666667	0.25			2	4	2	N/A	N/A	2.67	3
Accounting	0.5	0.222222222	0.75	0.4	0.6	3	2	4	2	3	2.80	3
Architects & Engineers	0.5	0.222222222	0.3125	0.4	0.4	3	2	2	2	2	2.20	2
Agriculture	0.25	0.222222222	0.25			2	2	2	N/A	N/A	2.00	2
Auto Dealers	0	0.666666667	0.25		0.2	N/A	4	2	N/A	1	2.33	2
Biotechnology / Life science	0.5	0.666666667	0.3125			3	4	2	N/A	N/A	3.00	3
Construction	0.125	0.222222222	0.25	0.2	0.2	1	2	2	1	1	1.40	1
Consulting Computer / Technology	0.5	0.666666667	0.4375	0.4	0.6	3	4	3	2	3	3.00	3
Data aggregators / Adminstrative	0.5	1				3	5	N/A	N/A	N/A	4.00	4
Educational institutions	0.25	1		1		2	5	N/A	5	N/A	4.00	4
Energy	0.25	0.666666667	0.25		1	2	4	2	N/A	5	3.25	3
Entertainment	0.5	0.222222222	0.25			3	2	2	N/A	N/A	2.33	2
Gaming / Gambling	1	1		0.8		5	5	N/A	4	N/A	4.67	5
Governmental related	0.5	1		1	0.8	3	5	N/A	5	4	4.25	4
Healthcare	0.875	1	0.875	0.6	0.8	5	5	5	3	4	4.40	4
Manufacturing	0.75	0.666666667	0.3125	0.2	0.6	4	4	2	1	3	2.80	3
Media, Printing & Publishing	0.75	0.222222222	0.25	0.4		4	2	2	2	N/A	2.50	3
Non-profits, membership organization	0.125	0.222222222	0.25			1	2	2	N/A	N/A	1.67	2
Real estate	0.5	0.222222222	0.25			3	2	2	N/A	N/A	2.33	2
Retail	0.75	1	0.75	0.6		4	5	4	3	N/A	4.00	4
Telecommunication	0.75	1	0.4375	0.2	0.2	4	5	3	1	1	2.80	3
Utilities	1	0.666666667	0.25	0.4	1	5	4	2	2	5	3.60	4
Wholesalers & Distributors	0.75	0.222222222	0.3125	0.4		4	2	2	2	N/A	2.50	3
Financial		0.222222222	1	0.6		N/A	2	5	5	N/A	3.33	3
Banking & Lending		0.222222222	1			N/A	2	5	N/A	N/A	3.50	4
Stock Exchange	0.75	1	1.00	1	1	4	5	5	5	5	4.80	5

Appendix C1 - Table 3

Revenue 1 000 000 000			
	Length 12	Length 18	Length 24
Hazard Class 5	5	10	9
Hazard Class 4	4	10	8
Hazard class 3	3	8	7
Hazard Class 2	2	2	5
Hazard Class 1	1	2	2
Revenue 500 000 000			
	Length 12	Length 18	Length 24
Hazard Class 5	N/A	4	9
Hazard Class 4	N/A	2	8
Hazard class 3	N/A	2	6
Hazard Class 2	N/A	2	5
Hazard Class 1	N/A	2	2
Revenue 250 000 000			
	Length 12	Length 18	Length 24
Hazard Class 5	N/A	N/A	2
Hazard Class 4	N/A	N/A	6
Hazard class 3	N/A	N/A	6
Hazard Class 2	N/A	N/A	2
Hazard Class 1	N/A	2	2