Differentiating Cyber Risk of Insurance Customers: The Insurance Company Perspective

Inger Tøndel, Fredrik Seehusen, Erlend Gjære, Marie Moe

Differentiating cyber risk of insurance customers: the insurance company perspective

Inger Anne Tøndel, Fredrik Seehusen, Erlend Andreas Gjære, and Marie Elisabeth Gaup Moe

SINTEF ICT, Trondheim, Norway
inger.a.tondel@sintef.no

Abstract. As a basis for offering policy and setting tariffs, cyber-insurance carriers need to assess the cyber risk of companies. This paper explores the challenges insurance companies face in assessing cyber risk, based on literature and interviews with representatives from insurers. The interview subjects represent insurance companies offering cyber-insurance in a market where this is a new and unknown product. They have limited historical data, with few examples of incidents leading to payout. This lack of experience and data, together with the need for an efficient sales process, highly impacts their approach to risk assessment. Two options for improving the ability to perform thorough yet efficient assessments of cyber risk are explored in this paper: basing analysis on reusable sector-specific risk models, and including managed security service providers (MSSPs) in the value chain.

Keywords: cyber-insurance; risk management; risk modeling

1 Introduction

Cyber-insurance has been defined in literature as *"the transfer of financial risk associated with network and computer incidents to a third party"* [9]. It can take many forms, offering third party or first party coverage, and covering a variety of threat types [8, 24]. The demand for this insurance product is increasing [35, 36]. Although cyber-insurance has been around in some form for several decades, the cyber-insurance products are still relatively immature. This is underlined by statements such as *"cyber policies are still the Wild West of insurance policies"* [11] and *"products are untested, pricing appears arbitrary and experimentation in contract writing is commonplace"* [4]. Academic research on cyber-insurance has identified a number of challenges and knowledge gaps [4, 24, 40], some of which are related to assessing cyber risk.

Taking on cyber in their product portfolio is associated with a greater risk for insurance companies than other traditional covers, which is reflected in the product's pricing. According to a UK study, the cost of cyber-insurance relative to the limit purchased is typically three times the cost of cover for more established general liability risks, and six times higher than for property insurance

[18]. The UK study additionally points out that cyber-insurance has a lower price differentiation across customers, something that may be due to a lack of historical data in underwriting or inappropriate means of assessing the cyber risk of potential customers. This is concerning as it undermines the role that insurance can have in increasing the security posture of insurance buyers, since they will not see any benefit in terms of lower insurance cost [18].

As a basis for offering policy and setting tariffs, cyber-insurance carriers need to assess the cyber risk of companies. Insurance companies do this to differentiate between potential clients, thus reducing the risk of adverse selection [34]. This paper explores the challenges insurance companies face in assessing cyber risk, based on literature (Section 2) and interviews with representatives from insurance companies (Section 3). Section 4 outlines two options for improving the ability to perform thorough, yet efficient assessments of cyber risk: basing analysis on reusable sector-specific risk models, and including managed security service providers (MSSPs) in the value chain. Section 5 discusses the contribution of the paper and provides suggestions for further work. Section 6 concludes the paper.

2 Known challenges for assessing cyber risk of insurance customers

A large number of standards, guidelines and research papers suggest methods for information security risk assessments [39]. Though they have their differences, the methods tend to include similar steps: characterisation of the system; threat and vulnerability assessment; risk determination; control identification, and; evaluation and implementation of controls [15]. Fig. 1 provides an overview of the risk assessment process and key challenges for insurance companies, identified through searches in academic literature as well as non-academic sources, such as news articles, technical reports and white papers (see Tøndel et al. [40] for more details on the method used for the literature study).

The cyber risk of an organisation depends on various internal and external conditions, including the organisation's assets, the technology they are using and its vulnerabilities, the security awareness and competence of the employees, routines relevant for cyber security, the security of the organisation's vendors, vulnerabilities in common infrastructure which the organisation relies on, and the motivation of potential attackers. With all these factors to consider, and limited knowledge of the impact of the various factors on the organisation's overall risk, risk is complex to understand and evaluate, and it is impossible to verify that the risk estimation is correct [24]. This is true for the organisation itself, but also for an insurance company offering cyber-insurance to the organisation. The premium paid by all insurance holders should cover any payouts plus return profit to the insurance company. To limit their own risk exposure, the insurers seek a mix of customers which provide a sufficient premium income compared to the overall risk portfolio, and a steady flow of payouts.

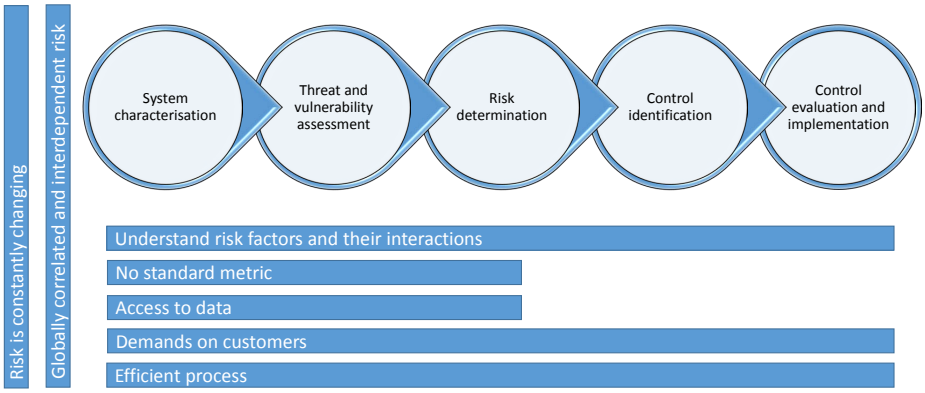

Fig. 1. The risk assessment process and challenges

The question of what constitutes "good IT security" has not been answered conclusively [13]. Research and practice on measuring information security has progressed, and there are many indicators and measurement frameworks available, see e.g. Herrmann [17] and ISO/IEC 27004 [20]. Still, there is no agreed set of metrics to predict information security risk in the general case [41]. Setting security baselines, or providing rewards for companies with documented security best practices, is difficult due to lack of knowledge about the effect of different security controls [26]. Simple metrics, like the number of records lost, does not always correlate with the total cost of the breach [30]. Currently, different insurance carriers evaluate risk in different ways, and they consider a variety of risk factors, covering both technical and organisational aspects [26, 27].

The lack of robust actuarial data has been pointed out by various sources as a reason for limited success of the cyber-insurance market [5, 13, 14, 41]. Several sources of historical cyber-incident information exist, e.g. from CERTs, security companies or researchers [13]. Examples of surveys that provide relevant data on costs of cyber-incidents are a NetDiligence survey of insurance payouts related to cyber liability [30] and Ponemon's Cost of Data Breach Study [37]. However, it is not easy to determine which sources of information should be relied upon more than others [13]. Barriers for information sharing include reluctance by firms to reveal details on security incidents [5, 16, 41], and limited ability to quantify costs associated with such incidents [41]. Toregas and Zahn make the following claim: *"Given that many companies are either unaware of a cyber attack or unwilling to disclose such attacks, and added to the fact that those attacks are hard to quantify, actuarial data for the cyber-insurance market is missing and unlikely to be available in the near future"* [41]. Insurance carriers are also reluctant to share incident information, due to a competitive market, and because they fear that they would ultimately *"give more than they get"* [26]. The significant information asymmetries currently present require insurance companies to perform costly state verification and upfront risk assessments [8].

Carriers engage clients heavily during the underwriting process. Historically they used extensive questionnaires [3, 27], but it is becoming more common to speak directly with clients to understand their vulnerabilities and risk management controls [27]. In this process customers may need to share a potentially large amount of information with the insurance company. It has been pointed out that in a competitive environment, potential customers may favour insurance companies with less demanding assessment processes [26]. Likewise, potential clients may not like being dictated by the insurance company on how to mitigate cyber risks [28]. Insurance companies are however also interested in having an efficient assessment process, illustrated by quotes such as *"carriers typically don't spend weeks with potential insureds reviewing every single aspect of an organization to see what's happening with its implementation of information security policies"* [26] and *"cybersecurity insurance underwriting essentially tries to weed out the 20 percent of companies who have no clue about cybersecurity from the pool of potential insureds"* [27]. Despite this need to have an efficient process, from the viewpoints of both customers and providers, it should be pointed out that the upfront risk assessment performed by insurance companies can have positive side-effects on increased self-protection, and the consulting and risk assessment services provided by the insurance company is one central driver of product value [8].

The experienced cyber risk may change rapidly based on technology changes, discovery of vulnerabilities, political actions etc. There is a need to understand how to take these changes into account when it comes to cyber-insurance. Organisational resilience, i.e. the capability of recognizing, adapting to and coping with the unexpected [42] is relevant for this. In the safety domain, research has progressed on measuring organisational resilience through risk awareness, response capacity and support [32], and such a measurement framework has been adapted to the ICT domain [7]. Rapid changes are additionally a challenge for collecting reliable actuarial data, as changes in technology and attacker profiles can cause empirical information on incidents to quickly become outdated [8, 24, 26].

According to Böhme and Schwartz [9], cyber risk is characterised by both interdependent security and correlated risk; the security of a node is dependent on the security of other nodes and incidents may strike in a correlated fashion. Interconnected nodes [3, 9] and dominant products [3] are key causes for this interdependency. An incident in one organisation may thus cause or increase the likelihood of incidents in another organisation. This risk comes in addition to the potential impact of an incident on third parties, up and down in the supply chain [10]. For insurance companies, these characteristics increase risk of concurrent claims [3]. Additionally, cyber incidents may cause pay-outs on a number of different insurance policies [22].

Table 1 gives a summary of key points from the literature related to these challenges.

3 Study of insurance companies

In addition to studying relevant literature, we have performed a study of experiences and practices of insurance companies when it comes to their cyber risk assessment of customers. The study reported in this paper is part of a bigger ongoing study with the overall goal of identifying what type of decision support and information is needed for evaluating cyber-insurance offerings, both from the perspectives of insurance companies and prospective customers.

3.1 Method

We have performed a study among key insurance companies offering cyber-insurance products in the Nordic market. The study included interviews performed in October/November 2015 and examination of relevant documentation. Relevant insurance companies for the study were identified by studying the web sites of such companies operating in the Nordic market, and the decision on which actors to approach for the study was based on the goal of covering the main actors in one country. The semi-structured interviews were carried out at the insurance companies' premises by one or two researchers, and the interviews were audio recorded and transcribed. The interview guide included the following topics: role of the interviewee; details of the cyber-insurance products offered; process for getting in touch with customers, evaluating risk and communicating policy terms to customers, and; future plans regarding cyber-insurance products. We talked with one representative from each company, and these were in underwriter or manager roles. Each interview lasted about one hour. All transcripts were thematically coded, and organised into thematic networks [2]. As the Nordic cyber-insurance market is small with a limited number of providers, we do not give any further details about the insurance companies that participated, in order to preserve anonymity. However, we point out that the number of companies interviewed is small, but still comprise the main actors in one of the Nordic countries. Regarding the context of the study, it should be noted that cyber-insurance is a relatively new product in the Nordics, and it is only the last few years that pure cyber-insurance products have been marketed here. Many Nordic companies are still unaware of cyber-insurance products' existence.

3.2 Results

The insurance companies we have studied seem to have relatively similar approaches to differentiate insurance customers in terms of risk. In general, they seem confident that their current approach and evaluation is good enough. At the same time they experience challenges and constraints in evaluating prospective customers' cyber risk. Fig. 2 provides an overview of the central themes that came up in the interviews related to assessment of risk. In the following we go into these in more detail. An overview of the findings, related to the challenges identified in literature, can be found in Table 1.

Challenge	Overview of state of the art	Interview study
Understand risk factors and their interaction; no standard metric	• Uncertainty in what factors are most important for risk [13, 24–26, 41]. • Challenging to achieve good measures of cyber risk [25, 33]. • Insurers lack experience and standards [24]. • Metrics considered by insurance companies are varied [3, 26, 27].	• No clear priorities on what risk factors are most important. • Do not have the competence in-house (use external security experts to perform assessments)
Access to data	• Lack of robust actuarial data is one reason for limited success of the cyber-insurance market [5, 13, 14, 41]. • Companies can be reluctant and unable to share reliable data on incidents [5, 16, 24, 25, 41]. • Cyber-incident cost is not clearly defined and hard to measure [5, 10, 24]. • A competitive environment hinders information sharing among providers [26, 27]. • Challenges of information asymmetry [3, 8, 9, 24].	• Cyber-insurance is a new product, i.e. having limited historical data to build on. • Getting hold of reliable data from customers can be challenging.
Demands on customers; efficient process for customers and insurance companies	• Clients may not like being dictated on how to mitigate cyber risk [24, 28], and may choose carriers with less stringent assessment practices [26]. • Insurance companies aim to reduce effort of assessments [3, 26, 27].	• Implementation of basic security measures is required, and risk assessment may introduce further requirements. • Large customer base is needed, thus also efficient risk assessment processes. • The sales process needs to be quick with a clear and easy-to-understand message.
Risk is constantly changing	• Rapid technological development and changes in attacker profiles may cause historical data to become outdated quickly [8, 24–26].	• It is challenging to stay updated in the field, things change quickly.
Globally correlated and interdependent risk	• Interdependent security and correlated risk; the security of a node is dependent on the security of other nodes and incidents may strike in a correlated fashion [3, 9, 24]. • Cyber incidents may cause pay-out on a number of different insurance policies [22].	• When concerned about catastrophic incidents, this impacts policy terms (become more risk averse).

Table 1. Overview of identified challenges from literature and interviews

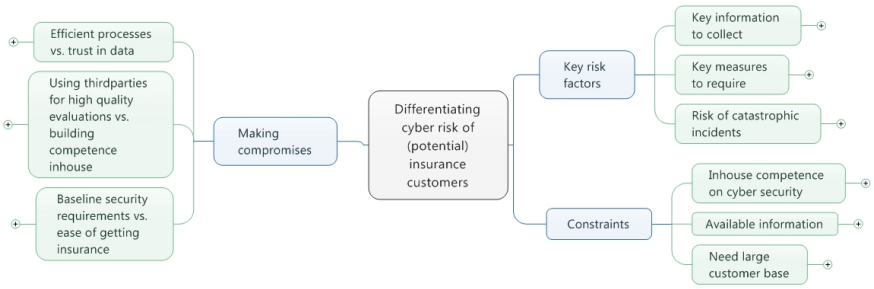

Fig. 2. Thematic network showing how insurance companies differentiate between potential customers.

Key risk factors. The interviewees did not provide any clear priorities on which risk factors they consider most important, except that commonly used factors include revenue and other metrics of the size of the business, as well as the organisation's operating sector. Instead, the insurance companies address a broad range of factors (e.g. based on the ISO/IEC 27001 standard [21]). They put some requirements on basic security measures that need to be in place for all customers, but they can also pose more specific requirements on individual customers. The criteria for deciding which security measures should be required from customers were not laid out by any of the interviewees.

Some of the interviewees are concerned about what could be called catastrophic risk, i.e. the risk of incidents which impact the majority of their customers at the same time. The interviews however give no indication of factors being considered most important to understand and address such risk.

Constraints. An interviewee explained how they find it challenging to stay updated on the field of cyber security. This may in part be related to the fact that cyber-insurance is a new product where they have limited experience and actuarial statistics to build on. But it is also pointed out that cyber security is an area where things change quickly, depending on the creativity of various threat actors.

Access to data is one challenge often experienced. The information most commonly collected (such as revenue and business sector) is easily obtained and trusted. However, other types of information (data protection is particularly mentioned) may be more difficult to get hold of. The interviewees mentioned a number of reasons for this: competence available in the business on cyber security and privacy; availability of the right people that have the competence, and; unwillingness to share information. In addition comes the risk of getting erroneous answers to the questions asked related to risk.

Insurance companies need to have a large customer base for their cyber-insurance products. This means that they need to be able to handle a large

number of customers in an efficient manner, but also that the sales process and the steps needed to become a customer is easy enough, not to hinder adoption. Additionally, the requirements regarding implementation of security measures must not be too strict. Currently, new customers are primarily reached through two channels (and this varies a bit between the insurance companies): insurance brokers and in-house sales personnel. Especially when in-house sales personnel are used, it seems important to exhibit a clear and easy-to-understand sales message and a quick process to sign up for cyber-insurance.

Making compromises. Today, insurance companies make several compromises in the process of evaluating risk, agreeing on policies and setting premiums. The following key areas came up in the interviews.

To get a large customer base, the insurance companies need to have efficient processes for evaluating risk and it must be easy for customers to buy insurance. At the same time, insurance companies need to be able to trust the assessments they make regarding cyber risk of customers, and thus need to get hold of a range of data related to risk. The collection process should ensure that data can be trusted. To achieve a balance between these needs, the insurance companies today differentiate their customers, and only perform thorough analysis of companies that are considered high risk. Differentiation is mainly done based on size, either of the company or of the amount insured. Small sized companies will have to answer only a very limited number of questions, ensuring the ability of the insurance company to reach and handle a mass of customers. For larger sized companies, a more thorough analysis is made, but also here some compromises have to be made to ensure an efficient collection process. Approaches made to data collection include questionnaires filled out by company representatives, interviews and security testing. Use of questionnaires requires less effort from the insurance company, but potentially at the cost of trust in the data. There is also the issue of how often to re-evaluate risk. The insurance companies are aware that cyber risk is dynamic over time. At the same time, they have limited capacity to re-evaluate risk on a regular basis.

The insurance companies in our study use third parties (cyber security experts) to perform the evaluation of company risks. Some interviewees state that a key reason for this is limited competence on cyber risk management in-house. The use of third party experts allows for high quality evaluations, and also opens possibility for learning from the third parties and thus gradually building more competence in-house. The insurance companies currently seem very dependent on the evaluations made by these third parties.

The insurance companies do put some baseline security requirements on their customers. As one interviewee states:"We don't want to insure a burning house!" At the same time, the companies want a volume of users, and to achieve this they cannot raise the bar too high for their customers. Currently, requirements on having anti-virus software and firewalls are common, either for becoming a customer or as part of the insurance terms. Insurance companies may have

more strict requirements for larger customers, based on the results of the risk evaluation.

4 Approaches to efficient and thorough risk assessments

The results from our interview study supports the current literature on risk assessment challenges for cyber-insurance carriers. The interview subjects all represent insurance companies offering cyber-insurance in a market where this is a new and unknown product. They have limited historical data to build on, and there has not been many incident cases yet. This lack of experience and data and the need for an efficient sales process highly impacts their approach to risk assessment. In the following we explore two options for being able to perform a thorough, and yet efficient assessment of risk in this context.

4.1 Reusable sector-specific risk models

As part of the process of differentiating cyber risk, insurance companies collect information from customers in a structured and repeatable manner, for instance through reusable questionnaires. We do, however, get the impression that the process of determining the appropriate risk level based on the collected information is not always structured, and can be based on expert judgement alone, which may result in arbitrary and poorly documented decisions. A common alternative to expert judgement is to use a *risk model*. A risk model is often specified in a modeling language that provides a precise and well-documented way of determining/calculating the risk level based on the information in the model. Creating risk models, however, can be time consuming, and making a new model from scratch for every assessment may not be feasible for insurance companies. One way of mitigating this problem is to create a generic risk model which captures some common knowledge and which can be reused in each assessment. Furthermore, the reusable risk model may be used as a basis for determining what kind of information should be collected from the customers.

In many settings, building a reusable risk model may not be worth it because the risk models vary too much across different assessments. However, in the setting of differentiating cyber risk insurance customers, several factors suggest that the use of reusable risk models may be appropriate: (1) The risk assessments have to be performed in a relatively short period of time, and the duration does not vary greatly from customer to customer. (2) The type of risks considered in each risk assessment are similar. These risks may for instance precisely correspond the type of cyber risks that are to be insured and which have precise legal definitions in the cyber-insurance terms and conditions, e.g. *Data Breach*, *Material Interruption*, or *System Failure*. (3) The information needed in each risk assessment is often collected from the customer in a structured manner and the type of information collected is similar across different customers.

In the field of risk assessment, several kinds of risk modeling techniques exists. These often build on tree-based and graph-based notations. Fault tree analysis

(FTA) [19], event tree analysis (ETA) [1] and attack trees [38] are examples of the former and provide support for reasoning about the sources and consequences of unwanted incidents, as well as their likelihoods. Cause-consequence analysis (CCA) [31], CORAS [23], and Bayesian networks [6] are examples of graph-based notations.

None of the above mentioned techniques have dedicated support for risk model reusability. In our opinion, for a risk modeling technique to support reusability, it should at a minimum: (1) Clearly distinguish between the information in the risk model which is *parameterized* (i.e. information that may vary across different risk model instances) and static information which should stay the same across different instances. (2) Provide clear guidelines for how the reusable risk model may be instantiated, i.e. how the parameterized information should be replaced with information specific to the instantiation domain.

Although none of the above mentioned risk modeling techniques have dedicated support for reusability, all of them can be extended to support this. One straightforward procedure for doing this in the setting of cyber risk insurance is as follows: (1) Make a risk model capturing general cyber attacks and cyber-insurance risks. (2) Identify and clearly mark which estimates in the risk model that are to be parameterized. (3) For each parameterized estimate, formulate a natural language question whose answer will allow the estimate to be determined for a given instantiation of the risk model.

By following the above steps, we obtain a set of questions in addition to a general risk model whose parametrized estimates are marked. To instantiate the risk model for a given cyber-insurance customer, we can give the questions to the customer, then determine the values of the parameterized estimates based on the answers to the questions, and finally determine the risk level using the guidelines of the risk modeling technique.

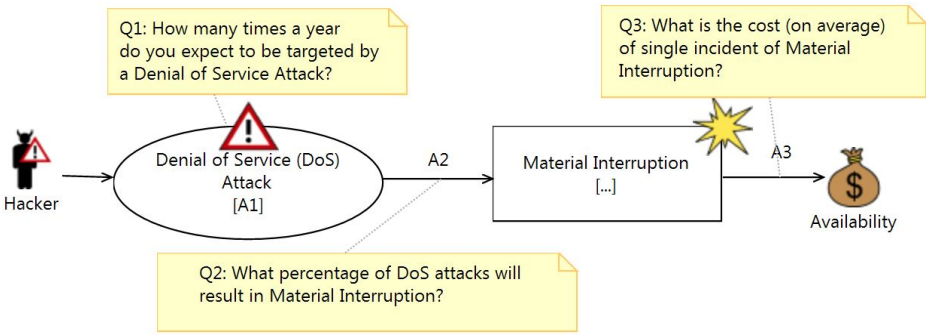

Fig. 3. Example of a reusable risk model specified in CORAS

As an example, consider the reusable risk model shown in Fig. 3 specified in the CORAS risk modeling language. A CORAS risk model is a graph whose nodes describe the occurrence of events, and whose edges describe causal rela-

tionships between events represented by the nodes. Nodes may be annotated with likelihood values specifying how often events occur, and edges may be annotated with conditional likelihood values specifying the likelihood that one event leads to another event given that the former event has occurred. Consequences may also be specified. In CORAS, this is done by including special nodes called *assets* (the money bag in Fig. 3). The consequence that a node has on the asset may then be specified by drawing an edge from the node to the asset and labelling the edge with a consequence value. The meaning of the risk model specified in Fig. 3 is: Threat *Hacker* initiates the threat scenario *Denial of Service (DoS) Attack* with likelihood $A1$ which leads to the unwanted incident *Material Interruption* with conditional likelihood $A2$ which impacts the asset *Availability* with consequence $A3$.

The CORAS modeling language does not have explicit support for specifying parameterized values. However, in Fig. 3, we have indicated the parameterized values by the variables $A1$, $A2$, and $A3$. In addition, we have specified questions that may help estimate these values. In particular, question $Q1$ will help estimate the likelihood $A1$ of DoS attacks, question $Q2$ will help determine the conditional likelihood $A2$ that a DoS attack will cause Material Interruption given that the attack is initiated, and $Q3$ will help estimate the consequence $A3$ of the Material Interruption risk if it occurs.

In general, mapping an answer to an estimate may not be straightforward. However, in the current example, this is fairly straightforward since the questions have been identified based on the risk model (as opposed to building an appropriate risk model from a set of questions). To make matters even easier (for the insurance company), the answers to the questions could be constrained such that they can be directly replaced with the estimates they help determine in the risk model. For instance, the possible answers to question $Q1$ could be a choice between the likelihood values *Low, Medium*, or *High*, whose values have been given a precise meaning, e.g. *Low* could mean less than one time per ten years. Note that the likelihood estimate of the unwanted incident Material Interruption in Fig. 3 is not parameterized. However, this likelihood value can be calculated based on the other likelihood estimates in the diagram using the CORAS likelihood calculation rules. Using the CORAS calculation and verification rules will not be an issue, since we are only interested in using these rules on *instances* of the reusable model after the parametrized estimates have been replaced by actual values.

Although there may be clear advantages of using reusable risk models to differentiate cyber risk of insurance customers, more research is needed to determine how well this would work in practice. A particular concern is the feasibility of providing estimates that are sufficiently precise to determine an accurate risk level. If this proves to be infeasible, a possible solution is to only use qualitative estimates, or to have an explicit representation of uncertainty in the risk model if quantitative estimates are used. Another concern is how often the models need to be updated or the risk re-assessed, due to the dynamic nature of cyber threats.

4.2 A role for managed security service providers

Involving companies known as *managed security service providers* (MSSPs) can potentially reduce the footprint and improve the quality of cyber risk assessments for insurance companies. MSSPs are security companies who provide a range of security products and services, often including 24/7 monitoring, analysis and detection of malicious network traffic. In addition to having clear knowledge of implemented security controls at their customers' site, MSSPs notify their customers about incidents as they happen and sometimes they assist customers further with incident response services. At the MSSP the incidents are continuously being documented over time, through a range of incident categories, both aggregated and on a per-incident basis.

From a perspective where the insurance company wants to assess risk of the customer when calculating a premium, we believe an MSSP engaged by the customer can provide very specific input in an effective manner, compared to existing alternatives and practices. The MSSPs have already insight into their customer's security architecture, strengths and weaknesses, and in particular the historical information on incidents and how these are handled. Such involvement mitigates the challenge on access to data, as identified in Table 1. In addition, MSSPs need to stay updated on general security and threat research, developing knowledge on the overall threat landscape including both public information as well as threat intelligence collected through monitoring their other customers, and through threat intelligence sharing channels. A partnership with an MSSP could help an insurance company better understand cyber risk, make the assessment process more efficient using previously collected knowledge, and staying up-to-date in terms of risk for the particular customer, general trends and globally correlated risks which may accumulate to catastrophic incidents.

For MSSPs and insurance companies to collaborate, incentives are needed for the customer organisation to allow information sharing between them. The MSSP holds very sensitive and detailed data about their customers, although some of this information can be made less sensitive through e.g. aggregation, anonymization or generalisation. Since MSSPs have their own security and risk experts in-house, the process of creating a risk map of their customer could for instance be offered as a service to the insurance company, without disclosing all of the underlying details. The result would still provide a reliable – and much richer – basis for the insurance company to assess risk, than simply relying on a self-evaluation by the customer.

While this approach limits the need for a potential insurance customer to expose sensitive information any further than already done, it also reduces their own workload related to obtaining insurance offers/coverage. It could also increase the likelihood that MSSP customers obtain a lower insurance premium as a result of implemented security measures, due to larger transparency for the insurance company and documented controls in form of the implemented security services by the MSSP. At the same time, selling this particular service provides an incentive for MSSPs to get involved in the value-chain, along with the potential upside for MSSPs on selling incident response services through insurance

companies whenever this serves as coverage. Finally, this process reduces costs for the insurance company since it would be less cost-demanding than employing another third party assessment from someone without previous knowledge of the potential customer's security architecture, controls and incident history.

If the MSSP industry were able to agree with the insurance companies on a standard for disclosing risk information about their customers, we believe a win-win situation could arise for all parties involved. In practice this is a matter of agreeing on a level of detail and a format of the information to be shared between the MSSPs and the insurance companies, and a portofolio of products they can collaborate on. It is an open question to insurance companies whether more transparency should automatically incur lower premiums. There could also be implemented mechanisms where the MSSP automatically alerts the insurance company directly about incidents at the insured company in a timely and standardised manner, making it easier for the insurance company to provide the right assistance in less time, and at an earlier stage, which may help in limiting costs of incident handling. One could also imagine that the MSSP would be directly authorised by the insurance company in these situations to implement mitigations within agreed coverage limits, which would likely be more effective than using a third party without a day-to-day relationship with the insured company.

5 Discussion

In this paper we have presented practice and challenges regarding assessing cyber risk of cyber-insurance customers, from the viewpoint of insurance companies. Practice and challenges have been identified by studying literature, and through a study of insurance companies in the Nordic market. It needs to be noted that the study of insurance companies reported in this paper only include a few companies, due to the size of the Nordic market, and in order to maintain their anonymity we do not provide any specific details on these companies. As a consequence of these limitations, we do not claim that our results are generalizable to all insurance companies. However, we believe the validity of our results is strengthened when considered together with known challenges identified in literature.

Table 1 compares the main results from the literature study with our study of insurance companies. The results are very much in line; the same challenges that are described in literature are experienced by the insurance companies we have studied. However, what is more of a concern for the companies that we have studied, compared to the emphasis it has been given in the literature, is the need for an easy to understand product and an efficient sales process. As already mentioned, the Nordic market for cyber-insurance is characterised by this being a new and unknown product. This impacts the approach taken to risk assessments. In addition to the need for an efficient sales process, the insurance companies have limited experience with the product and little historical data to

build on, though they can to some extent use experiences from cyber-insurance in other markets.

To improve cyber risk insurers' ability to have efficient, yet thorough analysis of cyber risk we have proposed two ways forward: reusable sector specific risk-models and including MSSPs in the value chain. These are not completely new ideas; the potential for developing a generic modeling structure for use with cyber-insurance has been discussed in a roundtable event organised by Department of Homeland Security [29] as part of their work with building a repository for sharing incident data [12], and in these discussions the potential role of security companies came up regularly when it comes to providing incident information [26–29]. The study we have performed further underlies the need for improved approaches, and in this paper we have provided more details on how one could go about building such re-usable models, and strengthen the input to the models by including MSSPs in the risk assessment process.

There is a need for more research in order to better understand how cyber risk assessments could be improved related to cyber-insurance. We have only studied this topic from the viewpoint of insurance companies, but other actors also have important roles in this respect; customers, brokers and third-party risk assessors. Further, the approaches we have outlined that can potentially improve current practice need to be evaluated to assess whether or not they will have the desired effect.

6 Conclusion

Insurance companies need to be able to assess cyber risk of prospective cyber-insurance customers. Many challenges related to performing such analysis have been identified in literature, and our study of insurance companies offering cyber-insurance to the Nordic market shows that these challenges described in the literature are relevant for insurers that operate in a market where cyber-insurance is a new and relatively unknown product. In such a market, the need for an efficient sales process and a clear sales message further constrains how insurance companies perform assessments of cyber risk. In this paper we have proposed two possible approaches to improve insurers' ability to perform efficient, yet thorough analysis of cyber risk: building reusable sector-specific risk models and collaborating with MSSPs.

Acknowledgments. This research has been performed as part of the inSecurance project, which is a strategic and internally funded research project at SINTEF ICT. We would like to thank the representatives from the insurance companies that participated in the interviews for sharing their experiences with us. We would also like to thank our colleagues Per Håkon Meland and Aida Omerovic for taking part in discussions leading up to this paper and for commenting on the interview guide, and our colleague Bjørnar Solhaug for performing and transcribing the interviews.

References

1. IEC 60300-3-9 Dependability management Part 3: Application guide Section 9: Risk analysis of technological systems Event Tree Analysis (ETA),
2. Attride-Stirling, J.: Thematic networks: an analytic tool for qualitative research. Qualitative research 1(3), 385–405 (2001)
3. Baer, W.S., Parkinson, A.: Cyberinsurance in IT security management. IEEE Security and Privacy 5(3), 50–56 (May 2007)
4. Bandyopadhyay, T., Shidore, S.: Towards a managerial decision framework for utilization of cyber insurance instruments in IT security. In: AMCIS 2011 Proceedings - All Submissions (2011)
5. Bandyopadhyay, T., Mookerjee, V.S., Rao, R.C.: Why IT managers don't go for cyber-insurance products. Commun. ACM 52(11), 68–73 (2009)
6. Ben-Gal, I.: Bayesian networks. Encyclopedia of statistics in quality and reliability (2007)
7. Bernsmed, K., Tøndel, I.A.: Forewarned is forearmed: Indicators for evaluating information security incident management. In: IT Security Incident Management and IT Forensics (IMF), 2013 Seventh International Conference on. pp. 3–14. IEEE (2013)
8. Biener, C., Eling, M., Wirfs, J.H.: Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice 40(1), 131–158 (2015)
9. Böhme, R., Schwartz, G.: Modeling cyber-insurance: Towards a unifying framework. In: Workshop on the Economics in Information Security (WEIS) (2012)
10. Cashell, B., Jackson, W.D., Jickling, M., Webel, B.: The economic impact of cyber-attacks. Tech. rep., CRS Report for Congress (April 2004)
11. Chickowski, E.: 10 things IT probably doesn't know about cyber insurance (September 23rd 2014)
12. Department of Homeland Security: Enhancing resilience through cyber incident data sharing and analysis: The value proposition for a cyber incident data repository. Tech. rep. (2015)
13. ENISA: Incentives and barriers of the cyber insurance market in europe. Tech. rep. (June 28th 2012)
14. EY: Mitigating cyber risk for insurers, part 2: Insights into cyber security and risk. Tech. rep., Ernst Young Global Limited (2014)
15. Fenz, S., Ekelhart, A.: Verification, validation, and evaluation in information security risk management. IEEE Security & Privacy (2), 58–65 (2010)
16. Gordon, L.A., Loeb, M.P., Sohail, T.: A framework for using insurance for cyber-risk management. Commun. ACM 46(3), 81–85 (Mar 2003)
17. Herrmann, D.S.: Complete Guide to Security and Privacy Metrics. Auerbach Publications (2007)
18. HM Government UK and Marsh Ltd.: UK cyber security: The role of insurance in managing and mitigating the risk (March 2015), `https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance`
19. International Electrotechnical Commission: IEC 61025 Fault Tree Analysis (1990)
20. International Organization for Standardization: ISO/IEC 27004: Information technology - Security techniques - Information security management - Measurement. ISO (2009)
21. International Organization for Standardization: ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. ISO (2013)

22. Lloyd's, Cambridge Centre for Risk Studies: Business blackout - the insurance implications of a cyber attack on the us power grid. Tech. rep., Lloyd's (2015)
23. Lund, M.S., Solhaug, B., Stølen, K.: Model-driven risk analysis: the CORAS approach. Springer Science & Business Media (2010)
24. Marotta, A., Martinelli, F., Nanni, S., Yautsiukhin, A.: A survey on cyber-insurance. Tech. Rep. IIT TR-17/2015, Ubstutyti du Ubfirnatuca e Telematica (2015)
25. Meland, P.H., Tøndel, I.A., Solhaug, B.: Mitigating risk with cyberinsurance. IEEE Security & Privacy (6), 38–43 (2015)
26. National Protection and Programs Directorate: Cybersecurity insurance workshop readout report. Tech. rep., U.S. Department of Homeland Security (2012)
27. National Protection and Programs Directorate: Cyber risk culture roundtable readout report. Tech. rep., Department of Homeland Security (2013)
28. National Protection and Programs Directorate: Cyber insurance roundtable readout report - health care and cyber risk management: Cost/benefit approaches. Tech. rep., Department of Homeland Security (2014)
29. National Protection and Programs Directorate: Insurance industry working session readout report. Tech. rep., Department of Homeland Security (2014)
30. NetDilgence: Netdiligence cyber claims study 2014. Tech. rep., NetDilligence (2014)
31. Nielsen, D.S.: The cause/consequence diagram method as a basis for quantitative accident analysis. Tech. rep., Danish Atomic Energy Commission, Risoe. Research Establishment (1971)
32. Øien, K., Massaiu, S., Tinmannsvik, R., Strseth, F.: Development of early warning indicators based on resilience engineering. In: PSAM10, International Probabilistic Safety Assessment and Management Conference. pp. 7–11
33. Oppliger, R.: Quantitative risk analysis in information security management: A modern fairy tale. IEEE Security & Privacy (6), 18–21 (2015)
34. Pal, R., Hui, P.: On differentiating cyber-insurance contracts a topological perspective. In: Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on. pp. 836–839. IEEE (2013)
35. Perlroth, N., Harris, E.A.: Cyberattack insurance a challenge for business (June 8th 2014)
36. Ponemon: Managing cyber security as a business risk: Cyber insurance in the digital age. Tech. rep., Ponemon Institute LLC (August 2013)
37. Ponemon: 2014 cost of data breach study: Global analysis. Tech. rep., Ponemon Institute LLC (May 2014)
38. Schneier, B.: Attack trees. Dr. Dobbs journal 24(12), 21–29 (1999)
39. Sulaman, S.M., Weyns, K., Höst, M.: A review of research on risk analysis methods for IT systems. In: Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering. pp. 86–96. ACM (2013)
40. Tøndel, I.A., Meland, P.H., Omerovic, A., Gjære, E.A., Solhaug, B.: Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research. Tech. Rep. SINTEF A27298, SINTEF (2015)
41. Toregas, C., Zahn, N.: Insurance for cyber attacks: The issue of setting premiums in context. Tech. rep., The George Washington University (January 7th 2014)
42. Woods, D.D.: Essential characteristics of resilience. Resilience engineering: concepts and precepts, Aldershot: Ashgate pp. 21–34 (2006)