SINTEF A27298- Unrestricted

Report

Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research

Authors
Inger Anne Tøndel
Per Håkon Meland
Aida Omerovic
Erlend Andreas Gjære
Bjørnar Solhaug

SINTEF ICT
Software Engineering, Safety and Security & Networked Systems and Services
2015-11-11

SINTEF IKT
SINTEF ICT

Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY

Telephone:+47
Telefax:+47 22067350

Enterprise /VAT No:
NO 948 007 029 MVA

SINTEF

SINTEF IKT
SINTEF ICT

Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY

Telephone:+47
Telefax:+47 22067350

Enterprise /VAT No:
NO 948 007 029 MVA

KEYWORDS:
cyber-insurance,
risk management,
cyber-incident impact

Report

Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research

VERSION 1.0	**DATE** 2015-11-11

AUTHORS
Inger Anne Tøndel
Per Håkon Meland
Aida Omerovic
Erlend Andreas Gjære
Bjørnar Solhaug

CLIENT SINTEF ICT	**CLIENT'S REF.** SEP InSecurance
PROJECT NO. 102009649	**NUMBER OF PAGES:** 24

ABSTRACT
Risk transfer can be an economically favorable way of handling security and privacy issues, but choosing this option indiscriminately and without proper knowledge is a risk in itself. This report provides an overview of knowledge gaps related to cyber-insurance as a risk management strategy. These are grouped into three high-level topics; cyber-insurance products, understanding and measuring risk and estimation of consequences. The topics are further divided into 11 knowledge areas with recommendations for further research. The work is based on a study of academic literature and other written materials, such as various reports and newspaper articles. There is a clear lack of empirical data on cyber-insurance, and in particular qualitative studies aiming to understand and describe needs, obstacles and processes relevant for cyber-insurance. We recommend a stronger emphasis on research related to topics that are specific to cyber-insurance, covering decision models for buyers of insurance, barriers for information sharing, impact of cyber-insurance on security, and business models for insurers.

PREPARED BY Inger Anne Tøndel	SIGNATURE Inger Anne Tøndel
CHECKED BY Martin Gilje Jaatun	SIGNATURE
APPROVED BY Bjørn Skjellaug	SIGNATURE

REPORT NO.	**ISBN**	**CLASSIFICATION**	**CLASSIFICATION THIS PAGE**
SINTEF A27298	978-82-14-05914-4	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
0.1	2015-10-26	Full version prepared for quality check
0.2	2015-11-09	Revision after quality check
1.0	2015-11-11	Final version

Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research

Inger Anne Tøndel, Per Håkon Meland, Aida Omerovic,
Erlend Andreas Gjære, and Bjørnar Solhaug

SINTEF ICT, Norway

Abstract. Risk transfer can be an economically favorable way of handling security and privacy issues, but choosing this option indiscriminately and without proper knowledge is a risk in itself. This report provides an overview of knowledge gaps related to cyber-insurance as a risk management strategy. These are grouped into three high-level topics; cyber-insurance products, understanding and measuring risk and estimation of consequences. The topics are further divided into 11 knowledge areas with recommendations for further research. The work is based on a study of academic literature and other written materials, such as various reports and newspaper articles. There is a clear lack of empirical data on cyber-insurance, and in particular qualitative studies aiming to understand and describe needs, obstacles and processes relevant for cyber-insurance. We recommend a stronger emphasis on research related to topics that are specific to cyber-insurance, covering decision models for buyers of insurance, barriers for information sharing, impact of cyber-insurance on security, and business models for insurers.

Keywords: cyber-insurance; risk management; cyber-incident impact

1 Introduction

Nearly all organizations are highly dependent on Information and Communication Technology (ICT) in their daily business. As a consequence, ICT incidents can affect organizations' ability to meet business goals. Security conscious organizations are aware of cyber-risks and take measures to reduce this risk. However, it is not possible nor economically feasible to protect against all eventualities. Thus, businesses can benefit from a mixed approach to cyber-risk management [50], taking into account a wide variety of risk reducing measures, including risk transfer in the form of cyber-insurance.

Cyber-insurance has been defined in literature as *"the transfer of financial risk associated with network and computer incidents to a third party"* [12]. A cyber-insurance policy can, for instance, cover liability issues, (digital) property loss and theft, data damage, loss of income from network outage and computer failures or web-site defacement [7], and is more specialized than traditional business interruption and crime insurances. Though cyber-insurance has been mentioned as a topic in the academic literature for more than two decades (see Böhme and Schwartz [12] for an overview of early works on cyber-insurance), 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"* [16] and *"products are untested, pricing appears arbitrary and experimentation in contract writing is commonplace"* [6]. The research on cyber-insurance is still in its early stages, and more knowledge is needed in various areas to support the development of improved cyber-insurance products, as well as to understand the impact cyber-insurance has on the security of organizations and society. Such research will moreover make a contribution to the more general field of the economics of information security [2] that started off at the turn of the century. The research field was triggered by the observation that misaligned incentives are as important as technical factors for explaining security failures [36].

This report provides an overview of knowledge gaps for cyber-insurance from the viewpoint of different actors, and describes the current level of knowledge in these areas. The motivation for providing such an overview is to support and guide future research in this field, and thus the report provides recommendations for research based on the identification of these knowledge gaps. The report is structured as follows. Section 2 explains the research method. Section 3 introduces the knowledge areas identified, while Sections 4 to 6 provide a more detailed explanation of the knowledge needs and the knowledge gaps. Section 7 provides recommendations for future research and discusses the validity of the work, while Section 8 concludes the report.

2 Research Method

In order to establish a baseline of the current state of cyber-insurance, we conducted an initial survey on the topic. We quickly discovered that the academic literature on cyber-insurance was not vast. To illustrate, a Scopus search in April 2015 using the search phrase (cyberinsurance OR "cyber insurance" OR "cyber risk insurance") resulted in only 40 hits (36 papers). Note that this search also covers the string "cyber-insurance" as it yields the same result as a search on "cyber insurance". In our work on identifying literature, we have thus also looked outside the academic literature and into news articles, technical reports and white papers. For the news articles we have prioritized recent publications in the period from October 2013 to April 2015. We also had to take into account that news articles tend to replicate each other or share the same source, so a large number of articles does not necessarily mean much novelty. This also meant that we could afford to miss several articles, so we do not claim to have full coverage of all news items published during our investigation period. Given the backgrounds and location of the authors, we were moreover limited to articles written in English or Norwegian.

Our survey work helped us identify key knowledge areas for cyber-insurance. This resulted in a list of 52 potential questions that we and the literature typically sought answers to. This list was then grouped (inductive, ground-up) into 14 themes. These themes were then considered together with research recommendations and cyber-insurance market barriers identified in two key reports [19, 56], and grouped into three main areas, with a total of 11 sub-areas.

In our work, we have primarily considered the risk-management aspects of organizations and their knowledge needs when considering cyber-security as one among several risk treatment strategies, as well as the needs of the insurance companies in evaluating the risk-level of potential clients.

3 Key knowledge areas when Considering Cyber-Insurance as a Risk Management Strategy

According to the widely established standard ISO/IEC 27005:2011 *Information security risk management* [30], there are four main strategies available for risk treatment: risk reduction, risk retention, risk avoidance and risk transfer. The four risk treatment strategies are not mutually exclusive, and organizations would usually benefit from using a mixed approach to risk management. Selecting an economically optimal mix of risk treatment strategies, however, is not trivial.

Businesses that want to utilize cyber-insurance as a risk management strategy need to understand the risk they are facing, and how cyber-insurance can reduce this risk. This implies a need to understand and evaluate cyber-insurance policies. Insurance companies, on the other hand, need to be able to differentiate between potential clients based on the risk they are facing, so as to reduce the risk of adverse selection [45]. They also need to understand the needs of the various market segments, in order to offer cyber-insurance products that are relevant. For both the supply and the demand side it is important to understand and document costs related to cyber-incidents, in order to agree on a compensation in case there is an incident.

In this report, the description of the knowledge areas for cyber-insurance has been divided into three high-level topics: cyber-insurance products (Section 4), understanding and measuring risk (Section 5) and estimate consequences (Section 6). An overview of the identified knowledge gaps is given in Table 1.

4 Cyber-Insurance Products (P)

Cyber-insurance can be offered according to various terms and be bundled in different ways. For the success of cyber-insurance, it is important that the products meet customer needs, and that there are adequate business models available for actors that have a role in offering insurance.

4.1 Take-up of cyber-insurance (P1)

Information about cyber-insurance uptake in different regions can contribute to understanding what makes cyber-insurance beneficial to stakeholders [19, 56]. Cyber-insurance is a relatively new product, even though there have been insurances covering *computer crime* since the 1980s [52]. Such predecessors of cyber-insurance were offered long before the existence of the Internet, covering, for example, losses due to fraudulent modification or destruction of electronic data. Given the criticality of ICT systems and the Internet of today, as well as the cyber-security issues they represent, the demand for cyber-insurance has increased, making the products more mainstream. According to Ernst & Young, nearly 60 insurers write some form of cyber-insurance coverage in addition to errors and omissions insurance [20]. However, it seems like there are great variations between the U.S. and Europe. Cyber-insurance is actually the fastest growing niche insurance product in the U.S. [46]. A study found that 31 % of businesses already have cyber-insurance policies, while another 39 % were planning to buy such policies in the near future [47].

As pointed out by Betterley [11], there were in Europe in 2012 only nine insurers with specialized cyber-insurance, compared to 30-40 in the US. According to ENISA [19] there is limited data on the size of the cyber-insurance market in Europe. A report from NSS Labs [13] states: *Interestingly, the market for cyber security insurance in the European Union is only a fraction of the current market in the United States. (The gross domestic product [GDP] of the EU is larger than that of the United States).* In Norway, the first pure cyber-insurance product was launched in 2015 [4], but there have been other products, such as generic crime insurances, that would cover some incidents related to cyber-crime. It is worth noting that a survey in the UK showed that less than 10 % of UK companies have cyber-insurance protection even though 52 % of CEOs believe that their companies have some form of coverage in place [35].

Looking at the market segments, the sectors typically buying cyber-insurance include retailers, health care providers, hotels and financial services [19] . These typically buy data breach insurances.

4.2 Government influence (P2)

Governments can, for example through regulations, influence the cyber-insurance market. This role should be well understood, both to avoid undesirable effects and to support initiatives that will improve overall cyber-security.

On February 12, 2013, the US President issued an executive order stating that the *cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront* [41]. In order to address this problem, one of the defined steps was to establish a Cyber Security Framework. The National Institute of Standards and Technology (NIST) was to engage cyber-security stakeholders, such as the insurance industry, in the creation of this framework. One of the expected outcomes here was a more competitive cyber-insurance market, and this can be seen as an example of how governments influence the market through direct order. In Europe, the proposed reform of data protection laws is expected to accelerate cyber-security insurance adoption in Europe. A similar thing happened in the US as a result of the state security breach notification laws [13].

In 2002, the US government passed the Terrorism Risk Insurance Act (TRIA), where the state acts as a re-insurance facility in case of a terrorist event that a normal insurance company would not be able to cover. This same model could be used for cyber-crime incidents with vast or catastrophic consequences to complete sectors or society, and across countries [19].

4.3 Evaluate cyber-insurance products (P3)

There is little information available on what factors are most important when deciding on whether or not to buy cyber-insurance. The Ponemon study [47] however provides some insight:

- 70 % of respondents reported that their company became more interested in cyber-insurance policies after experiencing an incident.
- Most companies believe that the cyber-security risk will either stay the same or increase, something that increases desire to purchase insurance.
- Those that do not plan to buy insurance provide the following main reasons for this: "Premiums are too expensive" (52 %) and "Too many exclusions, restrictions and uninsurable risks" (44 %).
- Those with a cyber-insurance policy, however, believe premiums are fair (62 %).

Another possible reason for deciding not to buy cyber-insurance is a perception that existing insurance, e.g., general business interruption policies, already cover cyber-risk [19]. In the Ponemon study [47] 38 % of those that did not plan to buy insurance provided the reason that "Property and casualty policies are sufficient".

SMEs are considered an important customer group for cyber-insurance, as SMEs in general have limited information security resources in-house [8]. Some insurance companies offer emergency response capacities to help deal with incidents, and for SMEs this may be more important than claims payout [8, 16]. However, the policies also differ in respect to what incidents are covered, the majority including incidents caused by human error or criminal attacks, but with less coverage for system failures or insiders and very limited coverage for attacks against business partners [47]. Policies may additionally exclude state sponsored cyber-attacks [19]. For organizations that have limited information security competence it may be difficult to understand the implications of such exclusions.

We are not aware of any empirical studies of the organizational processes that guide decisions on whether or not to buy cyber-insurance. Bandyopadhyay and Shidore [6] have proposed a decision model for cyber-insurance based on existing theoretical models of organizational decision making. In addition, Bandyopadhyay [5] has developed nine hypotheses on adoption of cyber-insurance by organizations. This is a good basis for performing empirical studies on cyber-insurance adoption.

4.4 Customer interaction (P4)

An essential question for prospective customers is of course how much they are willing to invest, both in the insurance, but also in the process of obtaining coverage. In order to set a premium, the customer needs to share a potentially large amount of information with the insurance company. According to Baer & Parkinson [3], an insurance underwriter may first ask prospective clients to complete an "Information Security Self Assessment", which could include information on a wide range of security controls such as configurations and security documentation for network infrastructure, information security policies, vulnerability monitoring, physical security and access controls, business continuity planning, periodic testing, etc. Depending on the extent of the insurance coverage and policy limits sought, further assessments may need to be performed by the insurer, including personal and physical inspections on the clients site. An independent third party which is specialized in information security could also be used to assess the customer. Since all such assessments are performed on a case-by-case basis [40], potentially comparable to a certification process along with the expertise needed to do them, the process comes with a potentially high cost [42]. Actual certificates, for example for ISO/IEC 2700x standards compliance, could in this respect provide companies a second-order advantage of being certified, both through cheaper insurance and as a low-effort way for insurers to be assured of a particular minimum level of security on the customer side. While there might be several relevant certifications that could be considered, and large enterprises are well familiar with certification and audit processes, any certification may be a barrier to undertake for smaller companies that also could constitute a significant market segment.

Interaction between insurer and the insured is needed also during the lifespan of the insurance. The customer could at any time take actions, not necessarily visible to the insurer, which have a positive or negative impact on the risk [3]. And if an incident occurs, at which point would the customer be required, for example, to notify the insurance company, when the timing here could have a significant impact on damages? Important questions include to what extent insurance holders are obliged to report on their actions, changes and incidents, and how they are incentivized to undertake precautionary measures if any loss is covered anyway. As such, buying insurance policies may just become an alternative to actually improving their security [57]. On the other hand, Toregas et al. [56] point out that differentiated premiums for high and low risk customers could be essential here to stimulate ICT security investments in parallel. It should be discussed how periodic checkpoints involving smaller audits or self assessments can be used to avoid worsening the information asymmetry and rather try to improve it over time, and allow insurers a correct impression of who are their high and low risk customers.

4.5 Business model for insurers (P5)

As with any insurance scheme, the premium paid by all insurance policy holders should cover any payouts plus return profit to the insurance company. As such, the insurers seek a mix of customers that provide a sufficient premium income compared to the overall risk portfolio, and a steady flow of payouts. This is especially a challenge for insurance companies in covering risk which may be globally correlated and interdependent [3]. Simultaneous attacks related to a specific operating system or software component, such as the Heartbleed bug [17], could quickly escalate into situations which reach catastrophic dimensions [19]. For these situations insurance companies normally have re-insurance, i.e. insurance for their obligations, which would cover them from potential bankruptcy. There are, however, still no re-insurers for cyber-insurance policies [56]. Hence, some policies exclude certain risks in this category from their coverage [20]. For the particular case of state sponsored cyber-attacks, it is an open question whether these should rather be covered by government re-insurance, such as the US Terrorism Risk Insurance Act (TRIA) [49]. Through being connected to a global Internet one is exposed to cyber-attacks originating from outside the national borders, and the question will arise of who is then responsible for re-insurance. There might also be differences between countries or regions in terms of culture and how damages are calculated.

An important perspective in this respect is which data will be part of the insured business, and how the data could potentially affect third parties. For example, if credit card information is stored, financial liability could be involved in the case of a breach, and coverage should be priced accordingly. This is in contrast to risk that only affects the first party, such as loss of profits through business interruptions or extortion [25]. The provisioning of insurance to third parties is an alternative to pay-outs that is currently being offered by some insurance companies, at least in the US [37]. A breach could, for example, expose customers of the insured, e.g. private individuals whose credit card numbers are stored in the breached system(s), and an identity theft insurance or credit monitoring services could for instance be provided to each of the affected individuals [40]. In contrast to traditional payouts which only have a cost, such cyber-liability coverage could rather extend the market reach for the insurance company. Worth noting is that there is supposedly no correlation between the number of records lost and the total cost of the breach [38].

5 Understanding and Measuring Risk (R)

For organizations, cyber-insurance is one of several risk-treatment strategies. Understanding the risk and the factors that influence the risk is important both to evaluate whether or not the risk is acceptable, and to what extent cyber-insurance can reduce the risk to an acceptable level. For insurance companies, understanding risk is important for differentiating policy terms and premiums, to prevent adverse selection [45].

5.1 Key risk influencing factors, and their relations (R1)

The risk to an organization is dependent on internal as well as external conditions. Central to the concept of risk is the assets of the organization and how vulnerable they are to threats. Internal factors influence the value of the asset as well as the risk, both negatively in form of errors/failures or insider attacks, and positively in form of implementing measures and contributing to resilience towards cyber-threats. Important internal risk influencing factors include the people working for the organization and their risk awareness and behavior, the technology the organization is using and its vulnerabilities and preventive measures, and how the organization is managed and the routines in place that are relevant when it comes to cyber-security. Organizations have a relatively high level of control over these internal risk influencing factors. However, in addition to internal factors, the risk is dependent on external factors over which the organization has more limited influence. Examples of external threats are failures of infrastructures that the organization relies on (examples could be communication network failures or power failures) and attacks by various attacker groups. Societal changes may also influence risk, in form of technology changes, political actions or public opinion. In addition, organizations typically rely on vendors, service providers or partners for various tasks. Cyber-incidents of such third parties may thus also have consequences for the organization, or vendors or partners may cause cyber-incidents in the organization itself. Getting insurance may influence the security work in the organizations, either positively or negatively (moral hazard [3]). With all these factors to consider, and limited knowledge of the impact of the various factors on the organization's experienced cyber-risk, risk is complex to understand and evaluate. This is true for the organization itself, but obviously also for an insurance company offering cyber-insurance to the organization (asymmetric information [12, 3]).

Risk modeling is a technique for risk identification and assessment, and the literature offers several tree-based and graph-based notations. Fault tree analysis (FTA) [28], event tree analysis (ETA) [29] and attack trees [53] 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) [39], CORAS [34], and Bayesian network [9] are examples of graph-based notations.

In the context of cyber-insurance, technological, organizational and human factors need to be modeled when assessing risk. Hence, expressiveness and scalability of the modeling approaches are crucial. While scalability is mainly concerned with the size of the eventual risk models, expressiveness is subject to what factors can be included in the model and reasoned about. The above mentioned approaches vary in these respects, as well as in their ability to model risk in terms of costs.

5.2 Measuring cyber-security in terms of costs (R2)

Risk modeling methods often lack techniques and tools for analyzing the associated cost and the return of investment of alternative risk treatments. Franqueira et al. [21] address this problem by proposing a method for handling security investment decisions achieved by so-called Real Option thinking. The method is partly based on Real Option Analysis (ROA) [1], which is a decision support technique in the area of capital investment by means of mathematical models to evaluate financial options. Other approaches to cost estimation in the setting of security investments are Net Present Value (NPV) [18], Return on Security Investment (ROSI) [54], Architecture Trade-Off Analysis Method (ATAM) [32], the Cost Benefit Analysis Method (CBAM) [31] and the Security Solution Design Trade-Off Analysis [27]. These and similar approaches can be understood as methods and techniques to facilitate security economics. In the context of cyber-insurance, two main criteria will be relevant for the choice of a cost modeling approach, namely dynamics of the cost over time, as well as availability of the input needed to estimate the needed model parameters. The above mentioned methods vary in this respect.

The eventual concern of risk management is how to provide the decision makers with an informed picture of the situation upon which they can confidently reason and act. When modelling risk, the main source of evidence is most often expert judgments, measurements and historical data. However, such empirical evidence are all characterized by a high degree of uncertainty. Research and practice on measuring information security has progressed, and there are many indicators and measurement frameworks available, see e.g. Herrmann [26] and ISO/IEC 27004. Still, there is no agreed upon set of metrics that are considered most important to predict information security risk in the general case [56].

5.3 Taking into account dynamics of technology and risk (R3)

The cyber-risk picture may change rapidly due to 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. Organizational resilience, i.e. the capability of recognizing, adapting to and coping with the unexpected [58], is thus relevant to consider. In the safety domain, research has progressed on measuring organizational resilience through risk awareness, response capacity and support [43], and such a measurement framework has been adapted to the ICT domain [10].

As a result of the rapid technological development and changes in attacker profiles, empirical information on incidents quickly becomes outdated. This increases uncertainty. When working quantitatively, a practical approach to take uncertainty into account, is in our experience to use intervals [24, 33, 44]. The intuition is then that the width of the interval specifies the level of uncertainty.

An interval is a special kind of distribution, namely the "flat" distribution. Theoretically, allowing also other kinds, such as Gaussian [14] distribution, would be preferable since this provides more information. Another relevant issue in the uncertainty handling is reliability and validity of the security assessment models. In other words, is the uncertainty of the models tolerable, and do the models sufficiently represent reality? Validity and reliability issues of security risk models have been elaborated on based on types of uncertainty representations, and based on the type of empirical input provided into the models. The problem in practice is to decide which approach to use and how. Comprehensibility is a major issue and performs differently among the various approaches. A simple, qualitative or frequency-based representation of the estimates is assumed to be generally more comprehensible than, for example, probabilities [22]. At the same time, the richer the representation, the more of the information available can be expressed with the needed precision.

6 Estimating Consequences of Cyber-Incidents (C)

Being able to estimate and measure the impact of cyber-incidents is important for both organizations and insurance companies: for setting premiums, for policy making, for making risk-based decisions on cyber-insurance, and for claims payout in case of an incident. Access to historical data on cyber-incident cost can improve ability to predict costs. Alternatively, the relationships between causes and effects of incidents need to be understood, so that costs can be modelled and estimated.

6.1 Historical data on cyber-incident costs (C1)

The lack of robust actuarial data has been pointed out by various sources as a reason for limited success of the cyber-insurance market [7, 19, 20, 56]. Barriers for information sharing include reluctance by firms to reveal details on security incidents [7, 23, 56] and limited ability to quantify costs associated with cyber-incidents [56]. 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"* [56] Various sources of historical cyber-incident information exist, e.g., from CERTs, profit companies or researchers [19]. Examples of surveys that provide relevant data on costs of cyber-incidents include a NetDiligence survey of insurance payouts related to cyber-liability [38] and Ponemon's Cost of Data Breach Study [48]. However, it is not easy to determine which sources of information should be relied upon more than the others [19]. To illustrate, the average cost reported for a breached record differs a lot between the 2014 versions of NetDiligence report and the Ponemon report; the NetDiligence study reports an average per record cost of $956.21 and a median cost of $19.84, while Ponemon reports an average cost for each lost or stolen record to be $145. There may be good reasons for these significant discrepancies in the numbers reported. An obvious reason is that the NetDiligence report reports only insurance payouts, and not the total cost of the incident. Also, the scopes of the surveys are different. Still, such large differences results in great uncertainties in what cost to expect, and it may be a cause to question the reliability of the data.

6.2 Models for understanding causes and effects of cyber-incidents (C2)

Bandyophyay et al. [7] divide costs of cyber-incidents into two broad categories: primary and secondary losses, where *primary* losses refer to direct loss and operating loss and *secondary* losses refer to any second-degree effects that are indirectly triggered by information concerning the security of the company (e.g., reputation damage or credit rating). ISO/IEC 27005 [30] in a similar fashion talks about immediate (operational) and future (business) effects. The *immediate* effects are then further divided into direct and indirect impacts. *Direct* impacts include cost of replacing the asset (acquisition, configuration, installation), the cost of suspended operation, and the experience of an information security breach. *Indirect* impacts include opportunity costs, cost of interrupted operations, potential misuse of the information, and violations of statutory or regulatory obligations as, well as ethical codes of conduct.

In general, cyber-incidents can have a long time span: the time between a vulnerability is introduced in the software till the vulnerability is exploited, and then till the attack is detected, can be quite long, and still it may take more time till the consequence of the incident is fully experienced. The immediate impact is relatively easy to identify, but indirect impacts and secondary losses may be difficult to fully understand, and they may also materialize long after the detection of the incident [15, 7]. Several factors may impact the costs. As an example, Bandyophyay et al. [7] explain how the decision to report the incident to an insurance company can increase the cost associated with the incident: the reporting may result in the breach becoming known to external parties, and thus secondary losses is experienced. Also, it is not always clear what costs are actually due to the incident. Cashell et al. [15] point out potential unclarities in this respect when it comes to direct costs (which are most likely the easiest type of costs to measure): *"If an attack leads to increased spending on IT security, to what extent are those costs attributable to the attack? If a planned upgrade in hardware or software is accelerated after an attack, should the upgrade be classified as a security cost?"* [15] Understanding and agreeing upon which consequences are actually due to an incident is likely to be more challenging for indirect and secondary losses.

According to Böhme and Schwartz [12], cyber-risk is characterized 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, 12] and dominant products [3] are key causes for this interdependency. An incident in one organization may thus cause or increase likelihood of incidents in another organization. This risk comes in addition to the potential impact of an incident on other firms up and down the supply chain [15]. These are not costs to the target organizations, and will thus usually not show in any cost estimates, but can still be severe. For insurance companies, these characteristics increases risk of concurrent claims [3].

The challenges of asymmetric information [12] also apply to cost estimation after a cyber-incident. Lack of understanding of costs, and in particular secondary losses, may result in overpriced contracts [7]. In addition, it is important that organizations understand what parts of the cyber-incident costs are covered by an insurance policy. Thus, adequate models for understanding cyber-incident impacts is important for a well-functioning cyber-insurance market.

6.3 Metrics and models for measuring costs of cyber-incidents (C3)

As the cost elements associated with cyber-incidents are not fully understood and agreed upon, different actors may have very different opinions on how incident costs should be measured. An insurance company would be concerned about arriving at reliable measures of the types of cost that is relevant for claims payout. Organizations would in addition be interested in getting an overview of the actual costs of an incident and what types of impacts that contribute most to the total costs, for input to risk management. Concerning cyber-insurance, organizations would benefit from an understanding of how much of the expected incident costs would actually be covered by a policy. This difference in focus is evident when looking at what cost items are considered in the NetDiligence survey of cyber-claims payouts [38] compared to the Ponemon study on costs of data breaches [48]. The claims payouts in the NetDiligence survey covered crisis service costs as well as legal and regulatory costs. The Ponemon study included detection and escalation costs, notification costs, post data breach costs and lost business costs. In most countries, lost business costs are the highest, with post data breach costs coming second and detection and escalation costs third. There is no direct mapping between the cost categories in the two studies, but for simplification and comparison you could say that the crisis service costs in the NetDiligence survey is mainly part of the escalation and notification costs in the Ponemon study, and that legal and regulatory costs are mainly part of the post data breach costs. Thus, major cost items identified in the Ponemon study seem to not be relevant for the claims payouts surveyed by the NetDiligence study.

When the cost items to be measured have been identified, it may still be challenging to come up with reliable metrics. The Ponemon study explains at a high level how they collect and calculate the costs of a data breach. The estimation of most of the costs is based on identifying activities, and then the companies estimate a cost for these activities. Examples of an activity can be *"Conducting investigations and forensics to determine the root cause of the data breach"* [48]. Then the activities are categorized into cost categories. For opportunity costs they estimate "turnover of existing customers" and "diminished customer acquisition" based on interviews with management. Though these measurement approaches are relevant and likely to result in useful data, they are prone to biases and are probably not reliable enough for claiming insurance payouts.

7 Discussion

In the following we make recommendations for further research and discuss the validity of these recommendations.

7.1 Recommendations for further research

Table 1 provides an overview of main knowledge gaps related to cyber-insurance, based on the above description of the identified knowledge areas. Clearly, there is a need for more research on several topics related to risk management, security-economics, business models, decision models and more. As an example, progress in understanding and measuring cyber-incident risk and cost in economic terms is very important for improving cyber-insurance products, as well as decision-making on whether or not to buy insurance. These are, however, active research fields of their own. Actors in the cyber-insurance domain would benefit from following the research in these fields so that the progress being made there can be used to improve the understanding of the cyber-insurance market and make a foundation for better cyber-insurance offerings. Still, the cyber-insurance research should address research questions that are specific for cyber-insurance. There is a need to understand the decision models used related to cyber-insurance, and what factors influence the demand for cyber-insurance products (P1,2,3). There is a need to understand the barriers for effective information sharing between insurance companies and organizations, so that these can be addressed in an effective manner (P4). And there is a need to understand how cyber-insurance impacts the security in the organizations and of society (P4,R1). There are also important challenges to be solved regarding business models for insurers (P5), especially when it comes to re-insurance opportunities.

As can be seen from Table 1 there is a need for improved models and methods, and probably also tools, related to cyber-insurance. At the same time, any such developments should be based on knowledge of the actual needs and challenges of the actors, and that any artifacts are properly evaluated to find whether or not they meet the needs. Today, there are some data available, mainly in form of statistics. In this report we have referred to statistics on incident costs [48], claims payouts [38] and cyber-insurance adoption [47]. Although there is a need for more and improved statistics related to cyber-insurance, there is also a need for more qualitative empirical research to increase understanding of these statistics. Such research is needed to understand both the demand and supply side of the cyber-insurance market. Important questions to study with respect to insurance companies are:

- What customer segment do you want to target with your cyber-insurance policies?
- What are the main obstacles with offering and selling cyber-insurance coverage? Why?
- What types of cyber-incidents are you most interested in issuing coverage for? Why?

Area	Knowledge gap
Cyber-insurance products	
P1	• What is the current uptake and market trends for cyber-insurance around the world? • What causes regional variations?
P2	• How are governments and other authorities influencing the market and role of cyber-insurance products? • How can governments act as re-insurer facilities for incidents with a global span?
P3	• What are the key differentiating factors for different customer groups when it comes to evaluating cyber-insurance offerings? • How are cyber-insurance decisions made in the organizations? • How can policy terms be communicated in an effective manner to those roles that are typically involved in making cyber-insurance decisions?
P4	• What information, and what amount of information, are businesses willing to provide to an insurance company, in order to obtain a cheaper premium — or to obtain insurance at all? • At which points should status and changes to the risk landscape be communicated between the insured party and the insurance company? • Will companies actually implement security improvements in order to obtain cheaper premiums, rather than simply rely on cyber-insurance alone? And how can insurance companies act to reduce moral hazard?
P5	• What private and public initiatives could address cyber-insurance market challenges, e.g., the lack of re-insurance? • What role could cyber-liability insurances play in the mix of cyber-insurance? • How will an insurance company deal with cases of extraordinarily high claims?
Understanding and measuring risk	
R1	• What are the key risk factors and their relations? • How does cyber-insurance influence the security of organizations, positively and negatively?
R2	• What standardized metrics are most useful for evaluating cyber-risk and cost? • How can methods for collecting and analyzing measurement data be improved to reduce measurement costs and increase reliability?
R3	• How can measurement frameworks and metrics sufficiently take into account changes in technology, business and environment?
Estimate consequences	
C1	• What actuarial data is most needed when it comes to cyber-incident costs? • How can such data be collected and made available in a manner that provides sufficient trust in the reliability of the data?
C2	• What are the key cyber-incident impact types? • What alternative criteria could be used for claiming that an effect is caused by an incident? • How can incidents be modeled in order to capture how various actions associated with an incident may impact the consequences of the incident, putting particular emphasis on the timing aspects?
C3	• What are current experiences and needs when it comes to measuring cyber-incident costs? • How can metrics for key cyber-security cost items be standardized?

Table 1. Identified knowledge gaps

- What cyber-insurance terms (what is insured, support in case of an incident, duration of policy, etc.) do you offer, and how and why have you decided on these terms?
- How do you deal with the timing issue of cyber-incidents (late detection, secondary impacts)? Why have you selected this approach? How easy is it to communicate with customers about these issues?
- What type of process would you prefer for customer segregation (evaluating risk, setting of premiums)? Why?
- Do you experience challenges regarding access to necessary information (relevant for risk analysis or for claims payout in case of incidents) from customers? Do you take any measures to increase willingness to share information with you? Why have you decided on those measures, and do they give the effect that you wanted?

For organizations that have bought an insurance, or have considered to buy insurance, important questions to address are:

- What motivates you to buy cyber-insurance? Why?
- If a vendor has been insured, how would that impact your evaluation of this vendor? Why?
- What characteristics of a cyber-insurance product makes it interesting for your organization? Why?
- What factors make a cyber-insurance product less attractive for your organization? Why?
- What types of cyber-incidents are you most interested in coverage for? Why?
- How do you experience the process of comparing different cyber-insurance offering? What makes it easy/hard?
- What decision basis and what decision process do you use when deciding whether or not to buy cyber-insurance? Should any aspect of this process be improved, and why?
- What type of benefits (size of claims payout, support, etc.) are important in case you experience an incident? Why?
- How willing is your organization to share security information with an insurance company? What can insurance companies do to increase willingness of organizations to share information with them?
- Is the work on cyber-security in your organization influenced by your decision to buy (or not buy) cyber-insurance? How, and to what extent?

Several research methods are available for qualitative research [51]. For studies that aim at understanding the viewpoint of several actors, we envision the use of qualitative interviews or focus groups [55]. For studies that want to go into detail on one or a few actors or products, case studies [59] would be a relevant research method, e.g. combining interviews, document studies and observations to provide a deeper understanding of the case studied.

7.2 Validity

In this report we have, based on a study of current literature related to cyber-insurance, identified a set of knowledge gaps, and provided suggestions for what type of research is most needed in the near future. Though we have collected information from various written sources, including both academic literature and other material, there is a possibility that we have missed relevant work. Still, we claim that our work provides a thorough overview of the current literature on using cyber-insurance as a risk management strategy.

Our review of the literature has identified a lack of empirical data on cyber-insurance. Due to this lack of empirical data it is difficult to know what are the different actors' needs when it comes to cyber-insurance. Thus, there is a limited basis for making prioritizations as to what knowledge gaps are most pressing to address. This impacts the validity of our conclusions. The need for more empirical data is real, but our recommendation to focus on cyber-insurance specific topics related to decision models, barriers for information sharing, impact on cyber-insurance on security, and business models, may be altered based on new empirical data becoming available.

8 Conclusion

This report has reviewed current literature related to cyber-insurance, and identified important knowledge gaps that need to be addressed to support a more effective cyber-insurance market. In particular, more empirical data is needed, both in form of qualitative and quantitative studies. While some quantitative data is already collected, we identify a need for qualitative studies that can provide more insight into the underlying factors and thus guide understanding of the quantitative data. We recommend that research should address cyber-insurance specific topics related to decision models, barriers for information sharing, impact on cyber-insurance on security, and business models. Still, improved knowledge on risk management and security economics is essential also for cyber-insurance, and the research in these fields should be followed closely by actors in the cyber-insurance domain to utilize the newest insights on understanding risk and cyber-incident in terms of cost.

Acknowledgments. The report is based on research funded by SINTEF ICT through the InSecurance project.

References

1. Amram, M., Kulatilaka, N.: Real Options:: Managing Strategic Investment in an Uncertain World. Oxford University Press (1998)
2. Anderson, R., Moore, T.: The economics of information security. Science 314(5799), 610–613 (2006)
3. Baer, W.S., Parkinson, A.: Cyberinsurance in IT security management. IEEE Security and Privacy 5(3), 50–56 (May 2007)
4. Bakken, J.: Vil forsikre Norge mot hacking. Online: `http://www.dn.no/tekno/2014/04/27/Finans/vil-forsikre-norge-mot-hacking` [Accessed October 26, 2015], in Norwegian

5. Bandyopadhyay, T.: Organizational adoption of cyber insurance instruments in IT security risk management - A modeling approach. In: Proceedings of the Southern Association for Information Systems Conference (SAIS'12) (2012), paper 5
6. Bandyopadhyay, T., Shidore, S.: Towards a managerial decision framework for utilization of cyber insurance instruments in IT security. In: Proceedings of the Seventeenth Americas Conference on Information Systems (AMCIS'11) – All Submissions (2011), paper 160
7. 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)
8. Barn, D.: Insuring cyber-assets. Computer Fraud & Security 2012(9), 5–8 (2012)
9. Ben-Gal, I.: Bayesian networks. In: Encyclopedia of Statistics in Quality and Reliability. Wiley (2007)
10. Bernsmed, K., Tøndel, I.A.: Forewarned is forearmed: Indicators for evaluating information security incident management. In: Seventh International Conference on IT Security Incident Management and IT Forensics (IMF'13). pp. 3–14. IEEE Computer Society (2013)
11. Betterley, R.: Cyber/privacy insurance market survey - 2012. Tech. rep., Betterley Risk Consultants, Inc. (June 2012)
12. Böhme, R., Schwartz, G.: Modeling cyber-insurance: Towards a unifying framework. In: Ninth Annual Workshop on the Economics in Information Security (WEIS'10) (2010)
13. Braunberg, A.: Multiple drivers for cyber security insurance. Tech. rep., NSS Labs (November 2013)
14. Casella, G., Berger, R.L.: Statistical Inference. Duxbury, 2 edn. (2002)
15. Cashell, B., Jackson, W.D., Jickling, M., Webel, B.: The economic impact of cyber-attacks. Tech. rep., CRS Report for Congress (April 2004)
16. Chickowski, E.: 10 things IT probably doesn't know about cyber insurance. Online: `http://www.darkreading.com/operations/10-things-it-probably-doesnt-know-about-cyber-insurance/d/d-id/1316862` [Accessed October 26, 2015]
17. Codenomicon: The Heartbleed Bug. Online: `http://heartbleed.com/` [Accessed October 26, 2015]
18. Daneva, M.: Applying real options thinking to information security in networked organizations. Tech. Rep. TR-CTIT-06-11, Centre for Telematics and Information Technology, University of Twente (2006)
19. ENISA: Incentives and barriers of the cyber insurance market in Europe. Tech. rep., European Network and Information Security Agency (2012)
20. EY: Mitigating cyber risk for insurers – Part 2: Insights into cyber security and risk. Tech. rep., EYGM Limited (2014)
21. Franqueira, V.N.L., Houmb, S.H., Daneva, M.: Using Real Option thinking to improve decision making in security investment. In: On the Move to Meaningful Internet Systems: OTM 2010, LNCS, vol. 6426, pp. 619–638. Springer (2010)
22. Gigerenzer, G.: Calculated risks – How to know when numbers deceive you. Simon & Schuster (2002)
23. Gordon, L.A., Loeb, M.P., Sohail, T.: A framework for using insurance for cyber-risk management. Commun. ACM 46(3), 81–85 (2003)
24. Heckerman, D., Mamdani, A., Wellman, M.P.: Real-world applications of Bayesian networks. Communications of the ACM 38(3), 24–26 (1995)
25. Hedrick, A.: Cyberinsurance: A risk management tool? In: Proceedings of the 4th Annual Conference on Information Security Curriculum Development (InfoSecCD'07). pp. 20:1–20:4. ACM, New York, NY, USA (2007)

26. Herrmann, D.S.: Complete Guide to Security and Privacy Metrics. Auerbach Publications (2007)
27. Houmb, S.H., Georg, G., France, R., Bieman, J.M., Jürjens, J.: Cost-benefit trade-off analysis using BBN for aspect-oriented risk-driven development. In: Proc. 10th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS'05). pp. 195–204. IEEE (2005)
28. International Electrotechnical Commission: IEC 61025 Fault Tree Analysis (FTA) (1990)
29. International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 31010 – Risk management – Risk assessment techniques (2009)
30. International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27005 – Information technology – Security techniques – Information security risk management (2011)
31. Kazman, R., Asundi, J., Klien, M.: Making architecture design decisions: An economic approach. Tech. Rep. CMU/SEI-2002-TR-035, ESC-TR-2002-035, Carnegie Mellon University (2002)
32. Kazman, R., Klein, M., Clements, P.: ATAM: Method for architecture evaluation. Tech. Rep. CMU/SEI-2000-TR-004, ESC-TR-2000-004, Carnegie Mellon University (2000)
33. Kearfott, R.B.: Interval computations: Introduction, uses, and resources. Euromath Bulletin 2(1), 95–112 (1996)
34. Lund, M.S., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer (2011)
35. Marsh: UK cyber security: The role of insurance in managing and mitigating the risk. Tech. rep., HM Government (2015)
36. Moore, T., Clayton, R., Ross, A.: The economics of online crime. Journal of Economic Perspectives 23(3), 3–20 (2009)
37. National Protection and Programs Directorate, U.S. Department of Homeland Security: Cybersecurity Insurance Workshop Redout Report (2012)
38. NetDilgence: NetDiligence Cyber Claims Study 2014. Tech. rep., NetDilligence (2014)
39. Nielsen, D.S.: The Cause/Consequence diagram method as basis for quantitative accident analysis. Tech. Rep. RISO-M-1374, Danish Atomic Energy Commission (1971)
40. Nordman, E.: CIPR newsletter: Managing cyber risks (2012)
41. Obama, B.: Improving critical infrastructure cybersecurity – Executive Order 13636 (2013), https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity
42. Ogut, H., Raghunathan, S., Menon, N.M.: Information security risk management through self-protection and insurance. Working paper at the University of Texas at Dallas (2005)
43. Øien, K., Massaiu, S., Tinmannsvik, R., Størseth, F.: Development of early warning indicators based on resilience engineering. In: 10th International Probabilistic Safety Assessment and Management Conference (PSAM'10). pp. 7–11 (2010)
44. Omerovic, A., Stølen, K.: A practical approach to uncertainty handling and estimate acquisition in model-based prediction of system quality. International Journal on Advances in Systems and Measurements 4(1 and 2), 55–70 (2011)
45. Pal, R., Hui, P.: On differentiating cyber-insurance contracts a topological perspective. In: IFIP/IEEE International Symposium on Integrated Network Management (IM'13). pp. 836–839. IEEE (2013)

46. Perlroth, N., Harris, E.A.: Cyberattack insurance a challenge for business. Online: http://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html?_r=0 [Accessed October 26, 2015]
47. Ponemon: Managing cyber security as a business risk: Cyber insurance in the digital age. Tech. rep., Ponemon Institute LLC (August 2013)
48. Ponemon: 2014 cost of data breach study: Global analysis. Tech. rep., Ponemon Institute LLC (May 2014)
49. President's Working Group on Financial Markets: Terrorism risk insurance (2006)
50. Refsdal, A., Solhaug, B., Stølen, K.: Cyber-Risk Management. Springer (2015)
51. Robinson, C.: Real World Research. Oxford, Blackwell, 3rd edn. (2011)
52. Schjølberg, S.: Cybercrime og forsikring. Nordisk Forsikringstidsskrift 2014(3) (2014), in Norwegian
53. Schneier, B.: Attack trees. Dr. Dobb's journal 24(12), 21–29 (1999)
54. Sonnenreich, W., Albanese, J., Stout, B.: Return on security investment (ROSI) - A practical quantitative model. Journal of Research and Practice in Information Technology 38(1), 45–56 (2006)
55. Stewart, D.W., Shamdasani, P.N.: Focus Groups: Theory and Practice. Sage Publications, 3rd edn. (2015)
56. Toregas, C., Zahn, N.: Insurance for cyber attacks: The issue of setting premiums in context. Tech. Rep. GW-CSPRI-2014-1, The George Washington University (2014)
57. Wheeler, J.: Security Think Tank: When cyber insurance is right and when it is not. Online: http://www.computerweekly.com/opinion/Security-Think-Tank-When-cyber-insurance-is-right-and-when-it-is-not [Accessed October 26, 2015]
58. Woods, D.D.: Essential characteristics of resilience. In: Hollnagel, E., Woods, D.D., Leveson, N. (eds.) Resilience Engineering: Concepts and Precepts, pp. 21–34. Ashgate (2006)
59. Yin, R.K.: Case Study Research: Design and Methods. Sage publications, 5th edn. (2014)