When to Treat Security Risks with Cyber Insurance

Per Håkon Meland[*+] and Fredrik Seehusen[*]

[*]*SINTEF Digital, Norway*
[+]*Norwegian University of Science and Technology, Norway*

ABSTRACT

Transferring security risk to a third party through cyber insurance is an unfamiliar playing field for a lot of organisations, and therefore many hesitate to make such investments. Indeed, there is a general need for affordable and practical ways of performing risk quantification when determining risk treatment options. To address this concern, we propose a lightweight, data-driven approach for organisations to evaluate their own need for cyber insurance. A generic risk model, populated with available industry averages, is used as a starting point. Individual organisations can instantiate this model to obtain a risk profile for themselves related to relevant cyber threats. The risk profile is then used together with a cyber insurance profile to estimate the benefit and as a basis for comparing offers from different insurance providers.

Keyword: Cyber insurance, risk quantification, risk profile, threats, decision making.

1 INTRODUCTION

Many organisations are now in the process of determining whether or not they should invest in cyber insurance. This is a new and challenging task for them, since there are not many established practices seen from the demand side. Though stand-alone cyber insurance products have been around for a couple of decades, they are still regarded as *"somewhat immature, with room for improvement"* (Hurtaud, Flamand, Vaissière, & Hounka, 2015).

For instance, varying form, content and vocabulary make it difficult to grasp coverage and terms, as well as compare policy offerings from different insurers (Meland, Tøndel, & Solhaug, 2015). Additional barriers have been explained by ENISA (ENISA, 2012), such that firms already think they are covered by their existing general business interruption policies. This optimistic belief of coverage was confirmed by a later UK study that MARSH published in 2015 (Maude, 2015). In 2016, a global study (Pain, Anchen, Bundt, Durand, & Schmitt, 2016) by Swiss RE and IBM Institute for Business Value concluded that the main reason why companies were not buying cyber insurance, was that they simply had not explored it.

The main contribution of this paper is a proposed assessment approach for organisations considering to buy cyber insurance. This is an investment decision that requires an understanding of cyber risk, but quantifying cyber risk is very challenging, even for large organisations with in-house security competence. Insurances are meant to take care of incidents that have low frequency and high impact, and single organisations are lacking historical data they can base their cost/benefit analysis on. At the same time, the technology, insurance market and threat picture are in constant development, making past experiences and data less valuable.

There have already been several publications covering various aspects for the demand side of cyber insurance. For instance, Gordon et al. (Gordon, Loeb, & Sohail, 2003) and Wang (Wang, 2017) provide frameworks for cyber risk management, where insurance is one of the means for risk reduction. Yannacopoulos et al. (Yannacopoulos, Lambrinoudakis, Gritzalis, Xanthopoulos, & Katsikas, 2008) discuss the level of coverage a firm should consider for privacy breaches given that the premium levels are set. Grossklags et al. (Grossklags, Christin, & Chuang, 2008) use game-theoretic models for shifting between investments in protection and self-insurance. They have showed that self-insurance may be more advantageous, especially when there are other firms that are more likely to be attacked due to weaker security. This model has been extended to also include market insurance by Johnson et al. (Johnson, Böhme, & Grossklags, 2011). Pal and Golubchik (Pal & Golubchik, 2010) have proposed a mathematical framework that co-operative and non-co-operative Internet users can exploit to balance defence investments with partial and full coverage insurance models. Böhme and Schwartz (Böhme & Schwartz, 2010) have developed a framework for modelling cyber insurance markets, which includes various attributes for cyber risk in relation to cyber insurance. Böhme and Schwartz also present a literature survey where both the demand and supply side are considered in this context. Later on,

Mukhopadhyay et al. (Mukhopadhyay, Chatterjee, Saha, Mahanti, & Sadhukhan, 2013) proposed another model to help firms decide upon cyber insurance, but with focus on utility for both the insurer and insured. A cyber risk profile for individual organisations is denoted by a unique utility function, and a Copula-aided Bayesian Belief Network (CBBN) model is used for assessing and quantifying the cyber risk.

Unlike the existing approaches, ours is initiated by a generic risk model that individual organisations can specialise to obtain a more optimal and tailored risk profile model for themselves. We assume that the organisations already have protection mechanisms in place, but want to reduce residual risk of rare events through cyber insurance. To evaluate the benefit of insuring, the risk profile is evaluated with and without a suitable insurance profile. The main advantages of this approach are that it makes use of available data concerning threats, likelihood and loss, and that it does not require the organisation to share information about their risks and incidents with external parties during the consideration phase. This should in turn make the organisation better equipped for negotiations with insurance agencies or agents.

This paper is structured as follows. The background and details of the approach are explained in Section 2. Section 3 discusses strengths and weaknesses, and section 4 provides a conclusion.

2 DESCRIPTION OF THE APPROACH

The development of the approach has been motivated by a Norwegian study (Meland, Tøndel, Moe, & Seehusen, 2017) on current practices for cyber insurance decision making. This study showed that obtaining a good understanding of cyber risk exposure is considered to be a critical, but also a very complex and challenging necessity. Risk managers and people with similar roles that already handle other types of insurance products within a company, typically do not know that much about cyber. Therefore, they find it difficult to perform cost/benefit analysis for cyber security, and to have a good and dynamic overview of the relevant threats. Another significant observation was that not all organisations are willing to share a lot of information about their security procedures, controls and incidents with arbitrary insurance agents, since they fear that this information could be leaked and damage their reputation or be exploited for attacks. There was also a general concern on how smaller organisations, lacking security competence and resources, will be able to make proper judgement on whether to buy cyber insurance or not.

The main target group of our approach is therefore organisations with limited in-house security expertise, that are considering investing in or renegotiating a cyber insurance policy. It has been the goal of our approach to be affordable, directly applicable for practitioners, and also to take advantage of available information. It is meant to accommodate specific industrial domains and improve over time as quantitative data becomes more reliable. We have used previous work from practical risk assessment (Tran, Solhaug, & Stølen, 2013), and adapted this to specifically address cyber insurance decision making.

The approach follows the steps as illustrated in Figure 1. The creation of a *generic risk model* is the first step, and is a collaborative task between security professionals, researchers and cyber underwriters. This risk model represents the typical threat events that a cyber insurance can cover, and what impact/consequences such events can lead to. The model includes sets of baseline data to be used as a starting point. The second step is performed by individual organisations to create a *risk profile* for themselves. The final step is the creation of a *cyber insurance profile*, which indicates cost reductions per threat in combination with the premium. The next sections explain these steps in more detail and with examples.

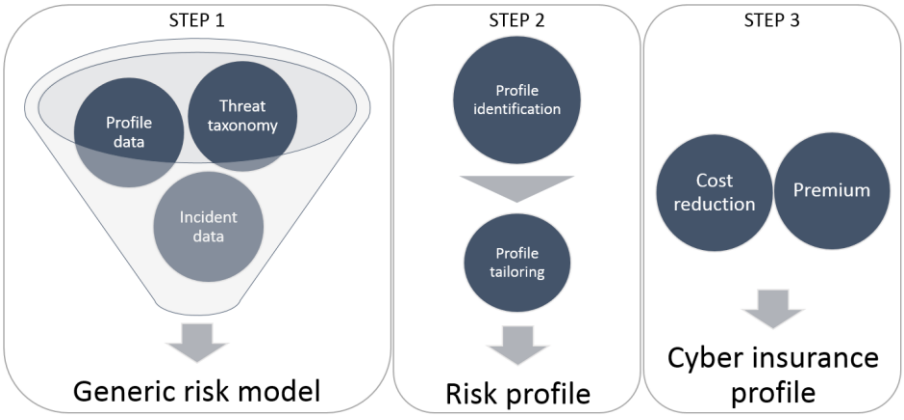

Figure 1. Approach overview.

Assembling a generic risk model

The purpose of this step is to define a risk model which is generic in the sense that it is parametrised by *company profiles*. A company profile is set of values such as size, location and industry that can be used in order to

categorise a given company. More precisely, a *generic risk model* is a triple (T, f, c) consisting of:

- A set of threats T;
- A generic frequency function f which takes a company profile cp as input and yields a mapping that for each threat t in T yields a frequency estimating how often incidents caused by t occur per year.
- A generic cost function c, which takes a company profile cp as input and yields a mapping that for each threat t in T yields the estimated cost of incidents caused by t.

The company specific *risk profile*, obtained from the generic risk model $M = (T, f, c)$ for a given company profile cp, is a triple (T_s, f_s, c_s) whose threats T are equal to the threats of M, and whose frequency and cost functions defined by $f_s = f(cp)$ and $c_s = c(cp)$ respectively.

We let rv be a function, which takes a frequency v_f and a consequence v_c and yields their *risk value* defined by their product, i.e. $rv(v_f, v_c) \triangleq v_f \cdot v_c$. The risk value of a given threat can be viewed as the *annual expected loss* due to incidents caused by this threat since we assume that frequencies estimate number of threat incidents *per year*.

In order to use the risk profile for determining whether or not to buy cyber insurance, we need to compute the total aggregated risk value, or the total annual expected loss due to all threats. We do not make any assumptions about overlap between threat incidents, i.e. whether the occurrence of one threat incident counts as an occurrence of an incident caused by another threat. For this reason, the total aggregated risk value is described by an interval, where the minimum interval value corresponds to the aggregated risk value in the case where there is the maximum possible overlap, and the maximum interval value corresponds to the case where there is the minimum possible overlap. More precisely, we define the total risk value of a risk profile (T_s, f_s, c_s) by the interval:

$$[rv(f_{min}, c_{min}), rv(f_{max}, c_{max})]$$

where

- f_{min} is the frequency for the case where there is a maximum possible overlap defined by the maximum frequency value $max(\{f_s(t) \mid t \in T_s\})$;
- f_{max} is the frequency for the case where there is no overlap defined

by the sum of all frequency values $\sum_{t \in T_s} f_s(t)$;

- c_{max} is the cost estimate of an arbitrary threat incident for the case where no overlap, defined by $(\sum_{t \in T_s} rv(f_s(t), c_s(t)))/f_{max}$;
- c_{min} is the cost estimate of an arbitrary threat incident for the case with overlap. The definition of c_{min} may depend on the risk profile. In this paper, we let c_{max} be an approximation of this cost, i.e. we let $c_{min} = c_{max}$. However, other definitions should be considered if this is not a reasonable approximation for the given risk profile.

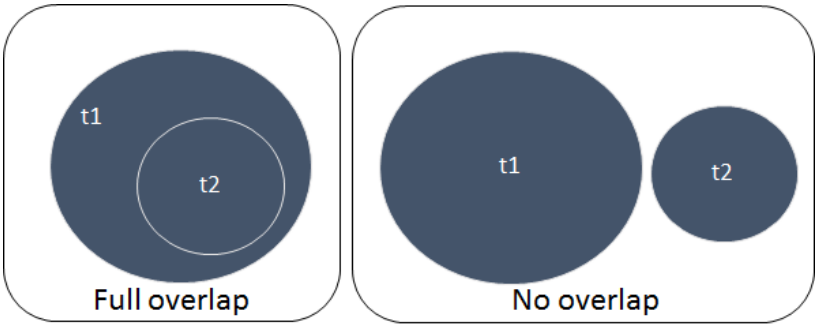

Figure 2 Full overlap: each incident caused by threat t2 also count as an incident caused by t1. No overlap: No incident caused by t2 count as an incident caused by t1.

Figure 2 illustrates what is meant by overlap. On the left-hand side, all incidents caused by threat t_2 also count as incidents caused by threat t_1. This is the case of maximum possible overlap which is assumed in the definition of f_{min}. Here, the combined frequency of the incidents caused by threats t_1 and t_2 is equal to the frequency of t_1, i.e. $f_{min} = max\{f_s(t_1), f_s(t_2)\} = f_s(t_1)$. On the right-hand side, there is no overlap, i.e. no incident caused by t_2 counts as an incident caused by t_1. This is the case of minimum possible overlap which is assumed in the definition of f_{max}. Here, the combined frequency of the incidents caused by threats t_1 and t_2 is equal to the sum of the frequencies of t_1 and t_2 , i.e. $f_{max} = f_s(t_1) + f_s(t_2)$. In this case, the total risk value is also equal to the sum of the risk value for each threat. This allows us to calculate the value of c_{max} as follows due to the definition of rv:

$$\begin{aligned} rv(f_{max}, c_{max}) &= rv\big(f_s(t_1), c_s(t_1)\big) + rv\big(f_s(t_2), c_s(t_2)\big) \\ f_{max} c_{max} &= rv\big(f_s(t_1), c_s(t_1)\big) + rv\big(f_s(t_2), c_s(t_2)\big) \\ c_{max} &= \big(rv\big(f_s(t_1), c_s(t_1)\big) + rv\big(f_s(t_2), c_s(t_2)\big)\big)/f_{max} \end{aligned}$$

In the continuation of this step, we include the following two activities for defining threats and profile type, based on data sources containing threat information, and for defining frequency and cost functions mapped to threats.

Define threats and profile type

The purpose of this activity is to define the set of threats and the possible company profile attributes of the generic risk model. The activity starts by identifying data sources that contain threat categories or taxonomies and statistics about threat occurrences and cost. After this has been done, a threat categorisation is selected from the data sources or created based on the data sources.

In our experience, nearly all data sources use different threat categorisations, thus creating a new unified categorisation is not straight forward. The data sources also tend to vary with respect to the detail and the kind of statistics they contain. Table 5 in the Data appendix gives an example of different threat categories from four different data sources.

As an example for this paper, we have chosen a threat categorisation from Advisen[1] as a basis for the generic model. This is not because we think its categorisation is the best, but because it seems to have the most detailed cost data. In addition to this, we have used data from Klahr et al. (Klahr, Amili, Shah, Button, & Wang, 2016) for estimating the likelihood of threat incidents. Advisen also contains data about how events (threat incidents) are distributed on different *industries*, and Klahr et al. contains data about the frequency of cyber breaches based on *company size*. In this paper, we will therefore consider company profiles based on size and industry. The Data appendix contains all the data material that we will use in this paper. Table 1 gives a definition of the threats T, as well as size S and industry I values considered in this paper.

[1]The dataset we have received from Advisen is dated November 2016 and contains 33023 cyber loss events. Romanosky has described the origin of this data in (Romanosky, 2016).

Table 1. Definition of threats T, size values S, and industry values I.

Name	Definition
T	Data - Malicious Breach; Privacy - Unauthorized Contact or Disclosure; Data - Physically Lost or Stolen; Data - Unintentional Disclosure; Network/Website Disruption; Privacy - Unauthorized Data Collection; Identity - Fraudulent Use/Account Access; Phishing, Spoofing, Social Engineering; Skimming, Physical Tampering; IT - Processing Errors; Undetermined/Other; Cyber Extortion; IT - Configuration/Implementation Errors; Industrial Controls & Operations
S	Micro; Small; Medium; Large
I	Services; Finance, Insurance and Real Estate; Public Administration; Wholesale and Retail Trade; Manufacturing; Transportation, Communications and Utilities; Mining and Construction; Agriculture, Forestry and Fishing

Define frequency and cost functions

The purpose of this activity is to define frequency and cost functions that map threats and company profiles to frequency and cost estimates. The definition should be made on the basis of the data that have been identified in the previous activity (which in our case is summarised in the *Data* appendix).

The definition of the frequency function f and the cost function c of our generic risk model are given in Table 2. Note that the available data material is not 100% applicable for defining the frequency and cost function that we need. For instance, the estimation of percentage of companies that have been breached due to a cyber threat is based on a survey in the UK (Klahr et al., 2016), and it may not be applicable for companies outside the UK. Another example is related to the cost data from Advisen, where it is unclear whether the data basis is a good representation of the entire population, and not for instance skewed to data mostly from the US, to big companies or to cyber events that are particularly costly. Indeed, the cost of

cyber events is estimated to be significantly higher in Advisen than in other studies from e.g. Kasperksy (Kaspersky, 2015) and particularly Klahr et.al. In the definitions, we implicitly assume that the data material used is applicable.

Table 2. Definition of the frequency and cost functions f and c (and helper functions) for the generic risk model.

Name	Definition	Description
$ei(i) \triangleq$	$ev(i)/26872$	Proportion of cyber incidents/events that occur in industry i. Here, $ev(i)$ denotes events recorded for industry i (the "Events" column in Table 7) and 26872 denotes the total number of recorded events (last row of Table 7).
$tp(t) \triangleq$	$ev(t)/33023$	The proportion of incidents that are caused by threat t. Here $ev(t)$ denotes the number of events/incidents recorded with respect to threat t according to Advisen (the "Events" column in Table 6) and 33023 is the total number of events recorded according to Advisen (last row of Table 6).
$b(s,i) \triangleq$	$\frac{b_s(s)ei(i)}{b_s(s)ei(i)+(1-b_s(s))si(i)}$	The likelihood of experiencing a threat incident within a one year period for a company with size s in industry i. Here, $b_s(s)$ denotes the proportion of companies of size s breached within a one year period (column "Proportion breached" in Table 9) and $si(i)$ denotes the relative size of the industry i (column "Relative size" in Table 10). We make the simplifying assumption that those companies that were breached, were breached only once, and that this breach counts as a single threat incident.
$f((s,i))(t)$	$\triangleq b(s,i) \cdot tp(t)$	The number of times per year that an incident caused by threat t occurs under the profile (s,i), i.e. for a company with size s in industry i.
$c((s,i))(t)$	$\triangleq evt(t)/tl(t)$	The expected cost of an incident caused by threat t under company profile (s,i). Here, $evt(t)$ denotes the number of events with recorded loss for threat t (corresponding to the "Events with loss" column in Table 6) and $tl(t)$ denotes total recorded loss (corresponding to the "Total loss" column in Table 6).

In Table 2, f and c are the generic frequency and cost mappings that given the company profile (s,i) yields a frequency and a cost mapping that is

specific to companies in industry i having size s. Both f and c are defined in terms of the other helper functions in Table 2. Of these, the definition of function $b(s,i)$ may not be immediately clear. This function is based on the function $b_s(s)$ which gives us the proportion of companies of size s breached within a one year period. However, what we want, and which is given by $b(s,i)$, is the proportion of companies of size s that were breached *provided* that they are in industry i. This is defined to be equal to the ratio of companies of size s in industry i that were breached $(b_s(s)ei(i))$ to companies of size s in industry i that were both breached *and not breached* $(b_s(s)ei(i) + (1 - b_s(s))si(i))$.

Tailoring an individual risk profile

The purpose of this step is to adapt the generic risk model to a particular organisation. Unlike the previous step, the intended user is a company or organisation that considers cyber insurance. The step has two activities, first a profile is identified and a corresponding risk profile is derived from the generic risk model. Then, this risk profile is manually refined by tailoring the frequency and cost values.

In the following, we will illustrate the step in an example for a fictive company we refer to as Acme, which is a medium sized company that provides an online marketplace where users can buy and sell goods and services from each other.

Table 3. The derived risk profile (second and third column) and the manually refined profile (fourth and fifth columns). Only the calculated risk value for the latter profile is shown.

Threat	*Frequency*	*Cost*	**Frequency**	**Cost**	**Risk value**
Data - Malicious Breach	*0.217*	*8538707*	0.217	8538707	1856717
Privacy - Unauthorized Contact or Disclosure	*0.116*	*5191220*	0.116	5191220	601702
Data - Physically Lost or Stolen	*0.076*	*983992*	0.000	983992	0
Data - Unintentional Disclosure	*0.074*	*1547339*	0.074	1547339	114929
Network/Website Disruption	*0.032*	*1327197*	1.000	100000	100000
Privacy - Unauthorized Data Collection	*0.012*	*1770338*	0.012	177033	21466
Identity - Fraudulent Use/Account Access	*0.012*	*3167541*	4.000	100000	400000
Phishing, Spoofing, Social Engineering	*0.011*	*40435298*	0.011	40435298	447775
Skimming, Physical Tampering	*0.011*	*1973479*	0.000	1973479	0

IT - Processing Errors	*0.007*	*92043291*	0.000	92043291	0
Undetermined/Other	*0.003*	*0*	0.000	0	0
Cyber Extortion	*0.003*	*92615*	0.003	92615	278
IT - Configuration/Implementation Errors	*0.003*	*12427442*	0.000	12427442	0
Industrial Controls & Operations	*0.001*	*42655*	0.000	4265	0
Total risk value/expected loss per year				**[2608007, 3542866]**	

Instantiate generic risk model

Based on the Acme profile (Size: *Medium* and Industry: *Services*) and the definition of our generic model, we can automatically derive the corresponding risk profile. This risk profile is shown in Table 3 in the first frequency and cost columns (column two and three). Here, the frequency value represents occurrences of the given threat incidents *per year* and the cost value represent the cost of threat incidents in USD.

The frequency and cost of each threat incident are calculated by the frequency function f and the cost function c defined in Table 2. For instance, the frequency for the threat $t =$ “Data - Malicious Breach", for company size $s =$“Medium" in industry $i =$“Services" is

$$f((s,i))(t) = b(s,i) \cdot tp(t) = 0.578 \cdot 0.376 = 0.217$$

Update metrics with own data (if any)

In this step, a domain expert can manually tailor the risk profile to her organisation. The procedure for this step is as follows: Walk through each threat, classify into one of the three categories described below, and adjust the frequency and cost accordingly. The three categories are:

- **Irrelevant threats**, i.e. threats that do not apply to the company, threats that are negligible, or threats that the company is not interested in insuring. Since the generic risk model is intended to capture all possible cyber threats, it will typically be the case that many of the threats are not relevant. For these threats, the frequency should be set to zero.
- **Familiar threats**, i.e. threats that have occurred in the past and/or occur on a regular basis. For these threats, the frequency should typically be increased, but the cost estimate should often be decreased, since the prior experience in dealing with these kinds of

threats contributes to lowering the cost. To avoid too much disalignment, adjustments in either direction can be based on the general prediction approach by Kahneman (Kahneman, 2011), which is used to adjust reference class averages with non-regressive intuitive predictions. In practice, the correlation between the risk profile attributes and the more specific attributes of the organisation can be used as a basis for this.

- **Unfamiliar threats**, i.e. threats for which there is no prior experience, but that could potentially occur. For these threats, the likelihood of the risk profile derived from the generic model provides a good starting point for frequency estimation, and should be kept unchanged if the company has no information about this threat. The same applies for the cost.

Continuing the example, we have shown the refined risk profile for the company in question in the second frequency and cost columns (the fourth and fifth columns) of Table 3. For Acme, physical attacks or unintended incidents are considered out of scope. The frequencies for threats in rows 3,9-11,13-14 have therefore been set to 0. Acme users buy and sell goods and services from each other, and fraudulent use of the service happens regularly i.e. about every four months. The typical attack vector is that the attacker is able to obtain the credentials of an end-user to the site by hacking the end-user directly. Hence, Acme is not directly responsible, but it could be *perceived* that way by the market. The cost is therefore not negligible, but not as high as in the derived risk profile. Acme experiences "Network/Website Disruption" from time to time, but these issues are covered by the service level agreement with the company that hosts the online marketplace, and the cost of these kind of incidents have been lower than in the derived profile. The frequency and cost of the remaining threats have been left unchanged. In Table 3, we can see that the threat with the highest risk value is "Data - Malicious Breach". This gives an indication of the types of threats that should be in focus when considering risk transfer to cyber insurance.

Creating a cyber insurance profile

Central to our approach, the decision on risk transfer should be based on a *cyber insurance profile*. A cyber insurance profile is a pair (cc, p) consisting of a cost cover function cc that takes a threat t as input and yields an estimate of how much of the cost of incidents caused by t will be covered by the insurance if they occur, and a cost p, the insurance premium, estimating the cost of insurance per year. These estimates must be determined based on a given insurance policy. The insurance premium is

often easy to determine, but the cost coverage can be more difficult to estimate as it also requires an understanding of the exclusions of the insurance policy. For a discussion of the kind of threats that are usually covered by cyber insurance, the reader is referred to (Meland et al., 2017).

Given a risk profile and an insurance profile, the *residual cost* of each threat t is obtained by subtracting the cost cover for t from the cost of t as specified in risk profile (setting the value to zero if the cost cover happens to be greater than the cost). We can then calculate a new (residual) total risk value based on the residual cost values. An insurance profile is *beneficial* if the total residual risk value with insurance plus the insurance premium is lower than the total risk value without insurance.

Table 4 gives an example of an insurance profile (column one and two), where we have assumed that the insurance covers the cost of each threat incident by 2500000 USD if they occur. Columns three and four in Table 4 shows the risk profile of our running example (Table 3) under this insurance profile. Here the cost of each threat incident has been reduced by 2500K USD, nullifying most of the residual risk values. The total residual risk value ranges from 1831796 USD to 2045122 USD. In the worst case, the benefit of this insurance profile is 562885 USD, i.e. the minimum total risk value of the risk profile without insurance minus the maximum total risk value of the risk profile with insurance (Table 4). Hence, in this case, the insurance would be beneficial if the premium is below 562885 USD per year.

Table 4. Example of a cost cover function (column one and two) of an insurance profile and a risk profile under this insurance profile (columns one, three, and four).

Threat	Cost cover	Frequency	Cost (res.)	Risk value (res.)
Data - Malicious Breach	2500K	0.217	6038707	1313099
Privacy - Unauthorized Contact or Disclosure	2500K	0.116	2691220	311933
Data - Physically Lost or Stolen	2500K	0.000	0	0
Data - Unintentional Disclosure	2500K	0.074	0	0
Network/Website Disruption	2500K	1.000	0	0
Privacy - Unauthorized Data Collection	2500K	0.012	0	0
Identity - Fraudulent Use/Account Access	2500K	4.000	0	0

Phishing, Spoofing, Social Engineering	2500K	0.011	37935298	420090
Skimming, Physical Tampering	2500K	0.000	0	0
IT - Processing Errors	2500K	0.000	89543291	0
Undetermined/Other	2500K	0.000	0	0
Cyber Extortion	2500K	0.003	0	0
IT - Configuration/Implementation Errors	2500K	0.000	9927442	0
Industrial Controls & Operations	2500K	0.000	0	0
Total residual risk value/expected loss per year			**[1831796, 2045122]**	

3 DISCUSSION

We have designed this approach to aid cyber insurance decision making based on the identified needs from a specific country (Meland et al., 2017). Still, we argue that this is transferable to other regions as well, since cyber threats are global, technology is converging and organisations seem to be facing the same barriers when dealing with cyber insurance.

Our notion of a risk model and risk profile is quite simple compared to other risk models we have already mentioned in the literature. First, we model likelihoods as real values representing frequencies of occurrence, but other notions of likelihood could have been possible. For instance, probabilities, intervals of probabilities or frequencies, or probability distributions. Second, we only model the likelihood that an incident caused by a threat occurs, and the cost of this incident if it occurs. However, it would also have been possible to model how often threat attacks occur, how likely it is that they succeed if they are carried out, what vulnerabilities could be exploited, what barriers are in place, etc.

There are three reasons why we have chosen to use the simple risk model. First, we are interested in defining a generic model which could apply to a large number of organisations, and we cannot rely on experiences from a particular organisation when estimating the likelihood and the cost of this model. We must therefore rely on threat statistics from available data sources in order to do the estimation. These statistics is often provided at a general level, and there is no unique and accepted source of information about e.g. economic magnitude (Eling & Wirfs, 2016), (Armin et al., 2015). For instance, it would be difficult to find an estimate of how often a particular kind of threat attack will succeed if it is carried out. Therefore, we have chosen not to include this in the risk model. The same reason applies for the way we have modelled frequency and cost. Using probability

distributions for both of these would have provided more analysis options, but finding the statistical data material available need to derive these distributions is difficult. Also pointed out by (Sigma, 2017), full probabilistic models are still in their infancy, and better cyber risk models will eventually emerge as understanding of the fundamental risk drivers develops and more data about cyber losses become available. Second, we aim to have a lightweight approach which is understandable for a non-expert, and which can be carried out in little time. The tailoring activity is meant to adjust for how the organisations perceive themselves compared to other businesses. Furthermore, the approach may be extended with more advanced utility functions for the demand side of cyber insurance, e.g. as suggested in (Mukhopadhyay, Saha, Mahanti, Chakrabarti, & Podder, 2005), (Böhme & Schwartz, 2010), (Eling & Wirfs, 2016) and (Wang, 2017) if needed. Third, the risk model is not intended to give a completely accurate description of the cyber risks for the organisation. Instead, it is meant to be used as a *guide* for the further steps in deciding whether or not to buy cyber insurance. Although our approach is based quantitative data, high accuracy is not important as long as it informs the decision making process. The approach can also be combined with the cyber insurance decision plan suggested by Gordon et al. (Gordon et al., 2003), which also includes steps for assessing insurance gaps, evaluating available policies, and selecting a specific policy. However, their work was published very early, and does not address that in practice, negotiations are used to tailor policy coverage and price to individual insurees instead of offering standard products (Hurtaud et al., 2015). To quote Siemens and Beck (Siemens & Beck, 2012); "*buying an off-the-shelf policy can result in disaster"*.

Regardless whether or not an organisation chooses to go forward with cyber insurance, this can only be part of the solution, and should not lead to negligence of security controls. In fact, there are significant cyber-related risks that remain largely uninsurable or the coverage is modest compared with the overall exposure (Sigma, 2017).

We have not defined as a part of our approach exactly *who* should be involved in the various steps for each organisation, since this will typically vary based on the size and type of the organisation, but an overview of suggested roles related to recommendations and decision is already given in a report from SANS (Filkins, Wright, & Bradford, 2016). A worrying finding from the same report, is that security professionals are rarely (28%) involved in the decision-making process leading to the purchase of cyber insurance.

For the continuation of our work, the generic model must be further developed, preferably with better measurement data, since we found a lot of deviations between different sources. Additional profile attributes and baseline values can be added, such as number of employees, system data (technological dependencies), GDP, geographic location, as well as an indication of risk appetite. Figure 3 illustrates what might be additional data ingredients going into the funnel.

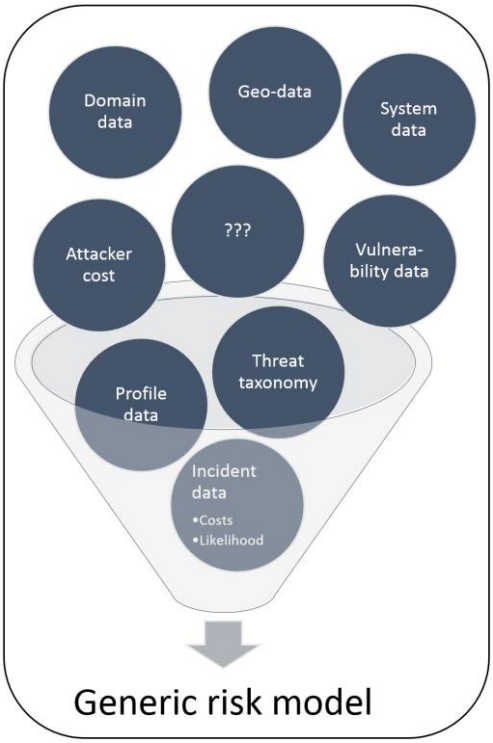

Figure 3. Possible additions of baseline data for the generic risk model.

A vast set of rating indicators for cyber insurance have been identified by Innerhofer-Oberperfler and Breu (Innerhofer-Oberperfler & Breu, 2010), but reference datasets must be made available in order to enrich the generic risk model and create more accurate risk profiles. We share the same positive opinion as Biener et al. (Biener, Eling, & Wirfs, 2015), that with increased marked development, we can expect better data sources as risk pools grow larger. Platforms for data sharing, organised by national regulators and international associations, should help keep this data accurate and updated to overcome the challenge of rapid technology development

and changing threat pictures. Even so, before increasing the complexity of the actuarial data, more systematic evaluations of the approach itself should be conducted, including a sensitivity study on the use of inaccurate data. We have so far received informal feedback during workshops with the insurance industry, and they appreciate the way risk models can be matched with insurance product to help their customers. Both insurers and insurees clearly share the common goal of better cyber security quantifications based on predictive, dynamic threat models.

4 CONCLUSION

We have observed that the demand side would like to have more practical help with deciding whether they need cyber insurance as a risk treatment option. Though several approaches for calculating insurance utility exist in the literature, they rely heavily on good input values for likelihood and costs/loss, and determining this is a great challenge for individual organisations. Our approach utilises available data sources to define a generic risk model, which is again tailored to the risk profile of individual organisations. The caveat here is that cyber event data will be quickly outdated and irrelevant if it is not updated and improved over time. We encourage the security and insurance community to make data about emerging threats and related costs available so that organisations can make informed decisions about risk treatment on a regular basis.

5 REFERENCES

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). 2020 cybercrime economic costs: No measure no solution. *10th international conference on availability, reliability and security (ARES),* (pp. 701-710). IEEE.

Biener, C., Eling, M., & Wirfs, J. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance*.

Böhme, R., & Schwartz, G. (2010). Modeling Cyber-Insurance : Towards A Unifying Framework. *Workshop on the Economics of Information Security*, 1-36.

Eling, M., & Wirfs, J. H. (2016). Cyber Risk: Too Big to Insure?--Risk Transfer Options for a Mercurial Risk Class. *I. VW Schriftenreihe, 59*.

ENISA. (2012). *Incentives and barriers of the cyber insurance market in Europe*.

Fidelity. (2016). *Quarterly Sector Update, forth quarter 2016*. Retrieved from https://www.fidelity.com/bin-public/060_www_fidelity_com/documents/Q4%202016%20Sector%20Update_Fidelity_FINAL.pdf

Filkins, B., Wright, B., & Bradford, D. (2016). *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey*.

Gordon, L., Loeb, M., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81-85.

Grossklags, J., Christin, N., & Chuang, J. (2008). Secure or insure?: a game-theoretic analysis of information security games. *Proceedings of the 17th international conference on World Wide Web*, (pp. 209-218). ACM.

Hurtaud, S., Flamand, T., Vaissière, L. d. l., & Hounka, A. (2015, February). Cyber Insurance as one element of the Cyber risk management strategy. *Inside magazine*.

Innerhofer-Oberperfler, F., & Breu, R. (2010). *Potential rating indicators for cyberinsurance: An exploratory qualitative study.* In *Economics of Information Security and Privacy* (pp. 249-278). Springer, Boston, MA.

Johnson, B., Böhme, R., & Grossklags, J. (2011). Security games with market insurance. *International Conference on Decision and Game Theory for Security* (pp. 117-130). Springer, Berlin, Heidelberg.

Kahneman, D. (2011). *Thinking, fast and slow*: Macmillan.

Kaspersky. (2015). *Damage Control: The Cost of Security Breaches IT Security Risks* Retrieved from https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Klahr, R., Amili, S., Shah, J. N., Button, M., & Wang, V. (2016). *Cyber Security Breaches Survey 2016*. Retrieved from https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016

Maude, F. (2015). *The role of insurance in managing and mitigating the risk*. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/uk-hm-government-and-marsh-cyber-security-role-insurance-managing-and-mitigating-risk

Meland, P. H., Tøndel, I. A., Moe, M., & Seehusen, F. (2017). *Facing Uncertainty in Cyber Insurance Policies*. Paper presented at the International Workshop on Security and Trust Management, (pp. 89-100). Springer, Cham.

Meland, P. H., Tøndel, I. A., & Solhaug, B. (2015). Mitigating risk with cyberinsurance. *IEEE Security & Privacy, 13(6), 38-43.*

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure {IT} or not? *Decision Support Systems, 56*, 11-26. doi:http://dx.doi.org/10.1016/j.dss.2013.04.004

Mukhopadhyay, A., Saha, D., Mahanti, A., Chakrabarti, B. B., & Podder, A. (2005). Insurance for cyber-risk: A utility model. *Decision, 32*, 153-170.

Pain, L. D., Anchen, J., Bundt, M., Durand, E., & Schmitt, M. (2016). *Cyber: In search of resilience in an interconnected world*. Retrieved from http://www.swissre.com/library/archive/Demand_for_cyber_insurance_on_the_rise_joint_Swiss_Re_IBM_study_shows.html

Pal, R., & Golubchik, L. (2010). Analyzing self-defense investments in internet security under cyber-insurance coverage. *30th International Conference on Distributed Computing Systems (ICDCS),* (pp. 339-347). IEEE.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2(2),* 121-135.doi:http://dx.doi.org/10.1093/cybsec/tyw001

Siemens, R., & Beck, D. (2012). How to buy cyber insurance. *Risk Management, 59*(8), 40.

Sigma. (2017). *Cyber: getting to grips with a complex risk*. Retrieved from http://www.swissre.com/library/sigma_01_2017_en.html

Tran, L. M. S., Solhaug, B., & Stølen, K. (2013). An Approach to Select Cost-Effective Risk Countermeasures. *Proceeding of 27th IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSEC'13),* (pp. 266-273). Springer, Berlin, Heidelberg.

Wang, S. (2017). Integrated Framework for Information Security Investment and Cyber Insurance.

Yannacopoulos, A. N., Lambrinoudakis, C., Gritzalis, S., Xanthopoulos, S. Z., & Katsikas, S. N. (2008). Modeling privacy insurance contracts and their utilization in risk management for ICT firms. In *European Symposium on Research in Computer Security* (pp. 207-222). Springer, Berlin, Heidelberg.

Data

Table 5. Examples of threat categories from the different data sources.

ENISA	**Advisen**	**Kaspersky**	**Klahr et.al.**
Malware	Data - Malicious Breach	Malware	Viruses, spyware or malware
Web-based attacks	Privacy - Unauthorized Contact or Disclosure	Phishing attacks	Other impersonating organisation in emails or online
line Web application attacks	Data - Physically Lost or Stolen	Accidental leaks/sharing of data by staff	Denial-of-service attacks
DoS/DDoS	Data - Unintentional Disclosure	Vulnerabilities / flaws in existing software	Access to computers, networks or services without permission (i.e. hacking)
Phishing	Network/Website Disruption	Network intrusion / hacking	Money stolen electronically
Insider threat	Privacy - Unauthorized Data Collection	Denial of service	Breaches from personally-owned devices
Cyber espionage	Identity - Fraudulent Use/Account Access	Loss/theft of mobile devices by staff	Personal information stolen
Ransomware	Phishing, Spoofing, Social Engineering	Intentional leaks / sharing of data by staff	Breaches from externally-hosted web services
Hacktivism	Skimming, Physical Tampering	Fraud by employees	Unlicensed or stolen software downloaded
ICS/SCADA hacking	IT - Processing Errors	Theft of mobile devices by external party	Money stolen via fraud emails of websites
Critical vulnerabilities	Undetermined/Other	Cyberespionage	Software damaged or stolen
Physical damage/theft/loss	Cyber Extortion	Security failure by third party supplier	Breaches on social media
Malicious code	IT - Configuration/Implementation Errors	Targeted attacks aimed specifically at our organisation / brand	Intellectual property theft
Botnets	Industrial Controls & Operations		

Table 6. Occurrences of threat incidents (events) and their loss measured in USD. Data source: Advisen.

Case Type	Events	Events with loss	Total loss
Data - Malicious Breach	12 410	622	$5 311 075K
Privacy - Unauthorized Contact or Disclosure	6 615	668	$3 467 735K
Data - Physically Lost or Stolen	4 347	80	$78 719K
Data - Unintentional Disclosure	4 239	102	$157 829K
Network/Website Disruption	1 824	115	$152 628K
Privacy - Unauthorized Data Collection	692	479	$847 992K
Identity - Fraudulent Use/Account Access	675	102	$323 089K
Phishing, Spoofing, Social Engineering	632	52	$2 102 635K
Skimming, Physical Tampering	623	84	$165 772K
IT - Processing Errors	390	41	$3 773 775K
Undetermined/Other	196	0	$0K
Cyber Extortion	171	153	$14 170K
IT - Configuration/Implementation Errors	168	19	$236 121K
Industrial Controls & Operations	41	2	$85K
Total	**33 023**	**2 519**	

Table 7. Occurrences of threat incidents distributed on industries. Data source: Advisen.

Industry	Events
Services	11 447
Finance, Insurance and Real Estate	5 633
Public Administration	4 142
Wholesale and Retail Trade	2 668
Manufacturing	1 508
Transportation, Communications and Utilities	1 238
Mining and Construction	202
Agriculture, Forestry and Fishing	34
Sum	**26 872**

Table 8. Industry sector size based in S\&P index. Data source: (Fidelity, 2016).

Sector size	Weight in S&P index
Consumer Discretionary	12.5
Consumer Staples	9.9
Energy	7.3
Financials	15.8
Health Care	14.7
Industrials	9.7

Information Technology	21.2
Materials	2.9
Telecommunication Services	2.6
Utilities	3.3

Table 9. Proportion of companies in the UK that have been breached in a period of 12 months. Data source: (Klahr et al., 2016).

Company type	Proportion breached
Micro	0.17
Small	0.33
Medium	0.51
Large	0.65
Overall	0.24

Derived data

The data in Table 10 has been derived by mapping the industry categorisation of Table 8 to the categorisation of Table 3 as follows:

- {Information Technology, Telecommunication Services, Health Care} ↦ Services
- {Financials} ↦ Finance, Insurance and Real Estate
- {} ↦ Public Administration
- {Consumer Discretionary, Consumer Staples} ↦
- Wholesale and Retail Trade
- {Industrials}↦Manufacturing
- {Energy, Utilities} ↦ Transportation, Communications and Utilities
- {Materials} ↦ Mining and Construction
- {} ↦ Agriculture, Forestry and Fishing

Note that the category “Public Administration" is not covered by the categories in Table 8. In the derived Table 10, we have assumed that this industry sector is 15% of the total. The relative size of the other industries in Table 10 are obtained by summing the percentages of their corresponding industries in Table 8 and multiplying by 0.85 (the proportion not covered by the Public Administration sector).

Table 10. Relative industry size.

Industry	Relative size
Services	32 %
Finance, Insurance and Real Estate	13 %

Public Administration	15 %
Wholesale and Retail Trade	19 %
Manufacturing	9 %
Transportation, Communications and Utilities	9 %
Mining and Construction	3 %
Agriculture, Forestry and Fishing	0 %

BIOGRAPHICAL NOTES

Per Håkon Meland is a senior research scientist at the independent research institute SINTEF in Norway. He obtained his MSc degree in Computer Science at the Norwegian University of Science and Technology in 2002, where he is also a PhD fellow in the intertwined fields of threat modelling and security economics.

Dr Fredrik Seehusen a scientist at the Norwegian Defence Research Establishment. He gained his PhD in computer science from the University of Oslo in 2009. He has previously worked at SINTEF in the areas of risk assessment, security testing, and formal methods.

AKNOWLEDGEMENTS

This research has been performed as part of the inSecurance project by SINTEF Digital. We would like to thank Professor Guttorm Sindre at NTNU for feedback, all the informants that participated in the interviews for sharing their experiences and needs with us, and representatives from brokers and insurance companies with whom we have been discussion this topic. This work has been partially funded by the EU-project WISER (653321).

REFERENCE

Reference to this paper should be made as follows: Meland, P.H. & Seehusen, F. (2018). When to Treat Security Risks with Cyber Insurance. *International Journal on Cyber Situational Awareness*, Vol. 3, No. 1, pp. 39-60.