Final published version is available from Springer: http://dx.doi.org/10.1007/978-3-319-68063-7_6

Facing uncertainty in cyber insurance policies

Per Håkon Meland[1,2], Inger Anne Tøndel[1,2], Marie Moe[2], and Fredrik Seehusen[2]

[1] Norwegian University of Science and Technology
{per.hakon.meland,inger.anne.tondel}@ntnu.no
[2] SINTEF Digital, Norway
{per.h.meland,inger.a.tondel,marie.moe,fredrik.seehusen}@sintef.no

Abstract. Cyber insurance has gained less ground in Europe than in the U.S., but with emerging laws and regulations, the prospect of considerable fines for security breaches is pushing many organisations into this market. A qualitative interview study in Norway reveals the main uncertainty factors for organisations that have little experience with the cyber insurance consideration process, and how they perceive the products, process and expected support in case of a cyber incident. These uncertainty factors can be reduced by being aware of typical coverage gaps, exclusions and loss types that are commonly found in cyber insurance products.

Keywords: cyber insurance; risk management; gap analysis; exclusions, coverage, negotiation

1 Introduction

Cyber insurance is an expanding market, fuelled by the growing number of cyber threats as our society becomes increasingly dependent on interconnected digital technology. In fact, Lloyd's City Risk Index [16] and the World Economic Forum [28] both consider cyber attacks to be one of the top risks facing the world today. Cyber insurance can be defined as the "transfer of financial risk associated with network and computer incidents to a third party" [5], and is meant to take care of incidents that have low frequency and high impact.

In the U.S., there is and has been a considerable up-take of cyber insurance. A recent survey by Hiscox [14] reports that 55% of U.S. respondents state they have cyber insurance. Looking at Europe, the situation is a bit different. According to a survey by Marsh & McLennan Co, only 13% of European companies have purchased this [19]. Why nine out of ten cyber insurance policies in the world are in the U.S., can probably be explained by more than ten years of state breach notification laws [7]. The situation is likely to become more similar in Europe, when emerging data protection regulations take effect in the near future [9]. For this reason, many organisations are now preparing to enter this market, but this is a new and challenging task for them, since there are not well-established practices for considering cyber insurance.

The main contribution of this paper is a study of the demand side view of cyber insurance, driven by the following research questions:

1. What are the main uncertainty factors in the consideration phase as perceived by the demand side?
2. How can these uncertainties be reduced?

Section 2 gives an overview over the related work for this topic. The former research question is studied in Section 3 through qualitative interviews with Norwegian organisations, who only have very little experience with this new type of product. For the latter research question, we analyse and discuss these uncertainties in Section 4 with experiences found in a more global perspective to see whether or not they are well-founded, and what can be done to reduce them. Section 5 provides a conclusion to the work.

2 Related work

There have already been several publications covering various challenges for the demand side of cyber insurance. Bandyopadhyay [2] have developed nine hypotheses on adoption of cyber insurance by organisations. He claims that organisations likely to adopt and utilise cyber insurance are recognized by high intensity of state of the art technology, business critical information systems, central management of cyber risks, efficient intra-organisational communication and collaboration, and imposed regulations. Those who are less accommodating typically have high security experience, high risk appetite, and a volatile business environment.

A survey by the Ponemon institute [21] provides some more empirical insight in which factors are most important when deciding whether or not to buy cyber insurance. For instance, 70 % of their respondents reported increasing interested in cyber-insurance policies after experiencing an incident. Among those that do not plan to buy insurance, the following main reason were given: "Premiums are too expensive" (52 %) and "Too many exclusions, restrictions and uninsurable risks" (44 %). Bandyopadhyay [3] has also argued that overpricing due to information asymmetry has been the primary reason for the limited growth of the cyber insurance market seen from the demand side. Additional barriers have been explained in separate studies by ENISA [12], U.S. Department of Homeland Security [23] and MARSH [17], such that firms already think they are covered by their existing general business interruption policies. Mr. Brew from Liberty International Underwriters [22] lists the following reasons why more customers do not buy cyber insurance:

- Cost and revenue concerns: Some see cyber security as a luxury purchase.
- Uncertainty: Will they actually pay out if there is an event? Untested market.
- High risk appetites: Technology entrepreneurs are risk takers, and do not see insurance as a necessary investment.
- Maturity: Companies are unaware of the availability of cyber insurance (and also about cyber security risk exposure).

A recent joint global study [20] by Swiss RE and IBM Institute for Business Value concluded with a very simple reason why companies were not buying cyber insurance; *they simply had not explored it*. This study included 1005 organisations from 15 industries in over 50 countries.

As can be seen from the literature, there can be many reasons why cyber insurance is still regarded as somewhat "immature, with room for improvement" [15]. The polices themselves tend to have varying form, content and vocabulary, which makes it difficult to grasp coverage and terms, as well as compare policy offerings from different insurers [18]. Though many organisations presumably seem to have taken an informed decision when deciding upon cyber insurance, a significant portion is also sitting on the fence because they do not feel competent to make any decision due to *uncertainty*. In the next section, we explore some of these uncertainty aspects in more detail.

3 Interview study

3.1 Method

During the autumn of 2016, we conducted a series of ten in-depth interviews with representatives from Norwegian organisations. Since only a very few Norwegian organisations currently have cyber insurance, the limited market made it difficult to design a larger empirical study. Still, we were able to obtain representation from different industries, such as finance, media, retail, critical infrastructure and IT. Most of these organisations are large by Norwegian standards, but a few were also medium size in the range of one hundred employees. Six out of the ten organisations had experience with a cyber insurance consideration process. Out of these, one organisation had acquired, two were still considering and three had decided not to invest in this option. The remaining four expressed their needs and thoughts if they were to start such a process.

We consider this setting to be representative for the Norwegian market and similar areas. Norway is considered to be technologically advanced and an example of a society that depends heavily on information systems, and thus, a society exposed to cyber threats. For instance, Norwegians use digital services to a large extent, well above EU average, and companies have a high on-line presence [10]. There is also a steady course towards a cashless economy where almost all transactions are done electronically [26]. Figure 1 illustrates a sample of digital maturity factors compared to the rest of Europe.

Each of the interviews lasted about one hour, and had a semi-structured form where one researcher asked the questions, and another made notes and additional remarks. All the results were also digitally recorded, transcribed and coded in a set of a priori main categories with emerging sub-categories. The complete results of the interviews are out of scope for this paper, but we have extracted the main uncertainty aspects with respect to *products*, consideration *process* and expected *support* in the case of an incident.

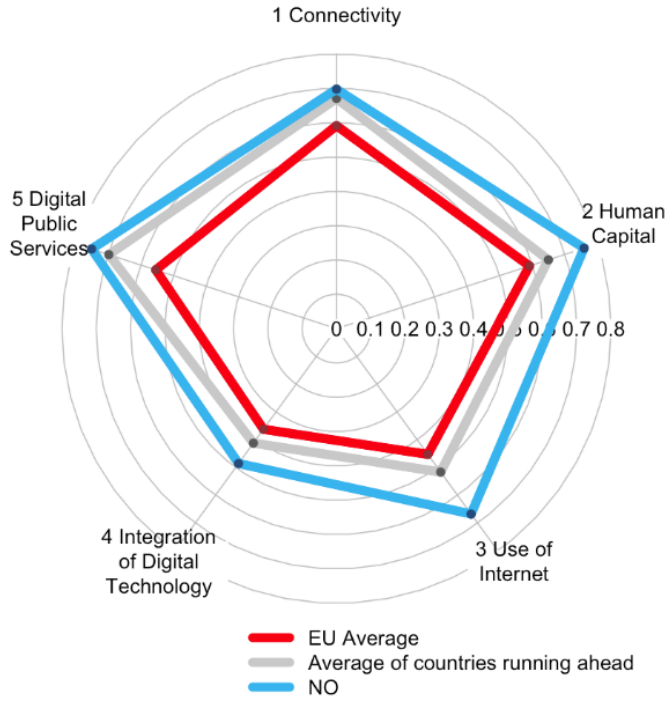

Fig. 1. The digital agenda scoreboard for Norway (2016) [10].

3.2 Results

Products In general, the cyber-insurance products and market are perceived as immature by those organisations that have considered to buy cyber-insurance. Characteristics put out by the informants include "there are different definitions to the term cyber risk", "the market is premature", "products are not prepared thoroughly", "there's lot of fancy words that we don't know the real meaning of". One informant had asked if their regular insurance company could provide this product for them, but they did not have anything readily available. In this case, the insurance company made one on-the-fly especially for this organisation.

The most important thing that make cyber insurance interesting seem to be coverage and limit. Price is less important. The informants seem to all agree that insurance is for catastrophes, that is incidents with high consequence and low likelihood. With today's cyber insurance products, coverage is perceived as low and not enough for to cover catastrophe costs. In addition, a cyber insurance will only cover parts of the real incident cost. Many of the companies we have talked to are mostly worried about reputation loss and loss of market position, and thus future income. Their impression was that these types of costs were not covered by an insurance. Many express that the cyber insurance products are

difficult to understand, and that many aspects are unclear, illustrated by quotes such as "for the time being, there is a lot of promise-ware" and "it is a product where it is not easy to get a concrete feeling of what is covered and not". Also, some informants were critical to the competence of the insurance companies in this field, mentioning: "When we asked technical questions about security, they could not really answer" and "... they don't know what they are selling".

There was a clear trend that the informants seemed unsure about the real benefits of the existing products. In addition, the products are perceived as expensive compared to other insurance products. One informant characterised the premium as "random", meaning it seems arbitrary what price you get based on the risk and the security measures of the company. This can be summed up by the following statement from one informant: "It is not everything that appears attractive and realistic for us to use. And the extent of coverage you will get in case of a break-in or an incident is a bit diffuse. They [insurance agents] say media support and so on, but what do they mean by that? It is very difficult to know the extent of that. In my opinion, the whole concept of cyber insurance is a bit vague and hard to grasp. The only thing that is concrete is the annual premium you have to pay".

Process When the organisations started the process of considering cyber insurance, the natural first step for them had been to assess their own cyber risk. Though most of the informants explain that their organisation already has some form of risk assessment practice that includes cyber, this does not seem to be enough to serve as a foundation for making decisions on whether or not to buy cyber coverage. Many of the organisations we talked to were still in the process of performing a more thorough risk assessment of their cyber risk, and a decision to buy cyber insurance was still pending from that assessment. However, as of now, they were still uncertain about their needs. The process of evaluating products was perceived complex and challenging for several reasons. First, as this is a new product, there is a general risk that no one picks up on it and takes responsibility for evaluating its relevance for the organisation ("it could easily fall between two stools").

Second, risk managers or similar roles that handle other types of insurance products do not know that much about cyber. Thus, they need more support from brokers than what is the case with most other types of insurance products. They also need to interact with IT people internally, something they are not used to, and this exposes them to a field very different from their own main competence. A few notable quotes from the interviews:

- "... it is a new area, and vague because you do not know enough about computers and do not have the fantasy to understand what is happening"
- "...sounded a bit like science fiction the first time I heard about it"
- "...you suddenly enter a technological world that is much more complicated than sitting and reading nice contracts"

Third, as explained before, products are perceived to be immature and terms are often unclear. It was stated: "Terms should be clearer than they are right

now. It seems that the insurance guys have just put up a list of things that would be nice to have. It does not say anything about at what level, and if there are any requirements on proof. Do we have to document all our security measures?" and "what does it mean to have a firewall or antivirus? What are the requirements to the firewall or antivirus? Does it e.g. have to be patched? What about gathering evidence after an incident? The policy does not say anything about this". Additionally, those that claim to know the cyber insurance market well, stated that this is developing rapidly, both when it comes to products and terms, and as a result, it is challenging to keep up to date.

Those companies with a lot of internal competence on insurance would actually prefer cyber as part of existing coverage, and not as a stand-alone product. One informant stated: "Then you can work with insurance companies that already know you, and it is cheaper". Another argued the following: "It is a small extension you do in an existing program, while buying a stand-alone product, which is offered on a broad scale, is a totally different scenario. There is extra work to for us to support them with their analysis, I'd rather work with those that already know our risk exposure".

As part of the negotiation with insurance companies, self-evaluation forms and questionnaires are frequency used. The organisations that have experience with these consider them to be relevant, but with the following remarks:

- "The form seems very high level, maybe because the policies are only meant to cover low pay-outs."
- "These forms are not suitable for complex, heterogeneous organisations, such as ours, with many locations for our different offices. There must be a dialogue."

One of the informant emphasised that their key success factor was obtaining a better understanding of the total risks that the organisation faced, and existing insurance coverage. This was stated as: "The most important thing we did in the beginning was this gap-analysis: what do we have, what do we lack when it comes to insurance". This was an activity in which they invested a lot of time together with their broker.

Support Though practical support from insurance companies in the case of an incident was not something most informants talked much about, there was an agreement on the following two things:

- It would be interesting to them if they would get access to highly specialised competence on the specific technology they are using.
- If such help should be useful, there must be a close relationship between the insurer and insuree over time, and an openness, "so they will know us and know how things are. They should not have to do a lot of research to understand us before they can start implementing countermeasures and limit damages".

Access to specialised competence and ability to have a close relationship were not something that the informants necessarily perceive to be part of current products, but something that would make the products more interesting. As of now, they are not sure if this is the kind of support that is offered. Additionally, there are uncertainties related to pay-out. This was related to lack of experience and unclear products (as explained above). One informant explained that they consider cyber insurance products to stem from the U.S. These [insurance] companies are perceived to have other ranges of pay-outs than what's common in Norway. This can impact the trust towards the product and process effort in case there is an incident.

4 Reducing uncertainty

A cyber insurance is not a silver bullet, and can never be a complete replacement for risk modification as a part of a risk management plan. Any organisation considering cyber insurance should focus on what kind of coverage they need to address their residual risk, and harmonise this with other insurances [13, 25]. But in order to do this, a lot of the uncertainty aspects from the previous section must be overcome. There is a lot of uncertainty related to the products themselves. Besides the novelty of the product, this is also caused by the fact that such policies are not standard products, but a result of a negotiation between the insuree and insurer. The negotiation phase is used to tailor standard products to more specific coverage and establish a price for individual insurees [15]. This includes defining exclusions, carve-backs, premium, payouts or support actions in the case of cyber events, cover limits (or caps), etc. To quote Siemens and Beck [25]; "buying an off-the-shelf policy can result in disaster". A negotiation would also be used when renewing policies, but for cyber insurance in particular, many organisations are doing this for the first time. The products themselves are therefore very much reliant on the process, and the support is a result of what has been agreed upon.

In the following sub-sections, we show what to be aware of when negotiating coverage of gaps, exclusions and loss.

4.1 Closing the gaps

A gap analysis for information security is usually performed to discover potential gaps between what level of security you have in place and requirements from regulations and standards, or in simple terms, *comparing where you are against where you want to be*. We noted from our interviews with Norwegian organisations, that when they were mentioning gap analysis, this was mainly about *determining whether or not the organisation was under-insured for cyber events*.

Most organisations already have a portfolio of insurance products in place, and general liability, property and crime insurances can in many cases cover a number of cyber events. However, they are not designed to fully cover all the potential costs and losses related to cyber risk [15]. In fact, there are significant

cyber-related risks that remain largely uninsurable or the coverage is modest compared with the overall exposure [27]. With little experience on claim from traditional insurances and cyber policies, there is a lot of uncertainty about loss coverage gaps. Therefore, it is important to have an idea of what risks are typically insurable and non-insurable, sort out the ones that can cover the needs, and prepare clarifying questions for the negotiation table.

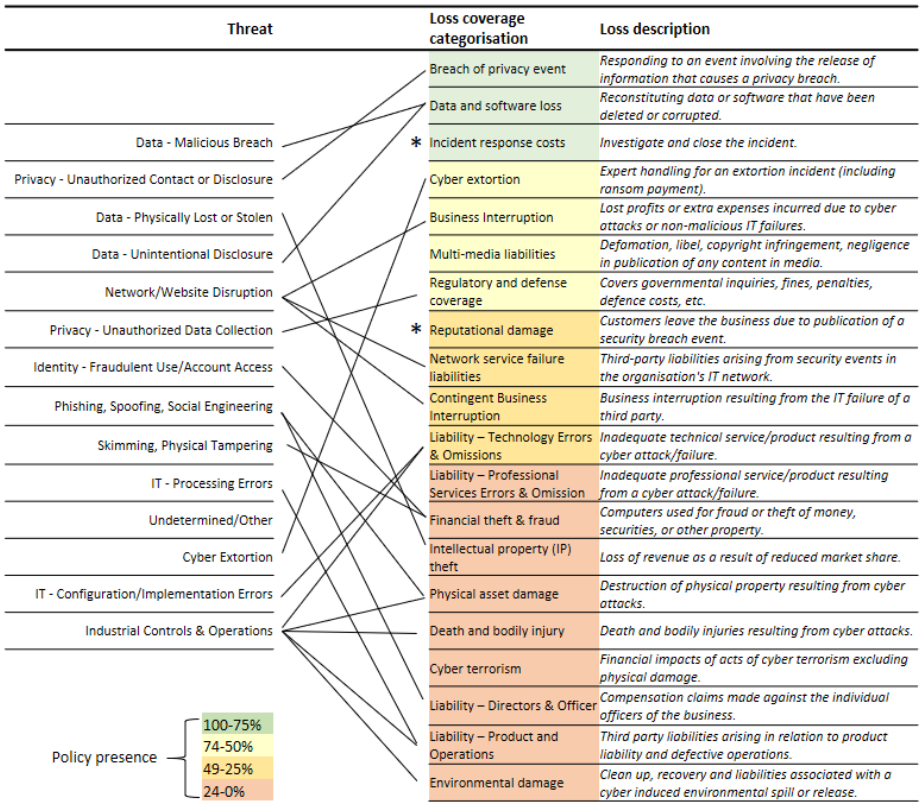

Fig. 2. Mapping between threats and loss coverage.

In Figure 2, we have combined two datasets to illustrate how cyber threats can be mapped to insurance coverage. The column to the left contains a threat categorisation from Advisen[3] ordered by registered loss amount. For instance, "Data - Malicious Breach" accounts for 622 cases with a total loss amount of $5,311,075K, while "Industrial Controls and Operations" accounts for merely two cases with a total of $85K. The rightmost two columns show typical loss coverage

[3] The dataset we have received from Advisen is dated November 2016 and contains 33023 world-wide cyber loss events. Romanosky has described the origins of this data in [24].

categories as defined in a study by Cambridge Centre for Risk Studies [6]. These 19 categories extend an original cyber loss categorisation scheme developed by a steering group of 15 insurance companies, several industry organisations and government agencies [17]. There was quite a variation on coverage in the 26 UK insurance products that was examined (two-thirds of what was estimated to be on the market). The colour scheme in Figure 2 indicates how commonly the losses were part of the policies. Due to the lack of an official vocabulary for cyber threats and losses, there is a significant degree of interpretation in this mapping, especially for the lower coverage segment. Also, note that a single threat category can lead to more than one type of loss. Especially "Incident response costs" and "Reputational damage" would have so many threat links that we did not include them in the figure.

In an ideal world, the most expensive threats would normally be present in cyber insurance policies, but as the figure shows, this is currently not the situation. It may also be that a policy contains coverage that is not relevant or necessary for the organisation that considers the insurance. It is therefore recommended to create an individual risk profile that can be used to compare expected threat exposure with what the policy offers to cover.

4.2 Checking for exclusions

It is typically in the lower coverage segment in Figure 2 that you will run into a world of exclusions that organisations must review, both for their existing policies and those under consideration. For instance, "cyber terrorism" is an ambiguous term, and probably more related to the people or group behind the threat, along with the associated motivation (e.g. political, religious, ideological or similar purposes), rather than the action itself. Many organisations would assume that any DDOS attack would be covered by Business Interruption, but according to [8], such claims could be rejected on the basis of a terrorism exclusion if there is a hacktivist group behind.

Besides war and terrorism exclusions, that are typically found in any type of insurance policy, there are exclusions that are particular for cyber insurance. The following check-list is based on reports from the Association of British Insurers [1] and Thomas Bentz from Holland & Knight [4]:

- **Court jurisdiction** - The territories of U.S. and Canada tend to be excluded from cyber insurance policies purchased in Europe.
- **Claims by related entities** - Claims related to loss of data belonging to employees (personal data), contractors and partial owned subsidiaries are not normally included.
- **Bodily injury and property damage** - As can be seen from the loss coverage categories in Figure 2, tangible assets tend to be excluded. General liability policies may already cover the direct expenditures, but probably not subsequent lawsuits.
- **Crime vs cyber insurance** - Consequences that are meant to be covered by a crime insurance policy, such as attacks leading to theft of money, will not

be reimbursed by a cyber insurance ("Financial theft & fraud" loss coverage category).
- **Mechanical/electronic failure** - Claims due to computers that stop working. Should be limited to malicious acts causing the computers to fail for the policy to respond.
- **Laptop exclusions** - Coverage for portable electronic devices tends to be excluded, especially if they do not encrypt their contained data.
- **Patent, software, copyright infringement** - We have already seen that IP theft belong to the lower coverage segment. Carve-backs (exclusion overrides) can be negotiated to cover claims caused by non-management employees and third parties.
- **Employment practices** - Incident arising from poor or insecure employment processes are often excluded or can shrink the policy's limits.
- **Employee benefit plan breaches** - Often referred to ERISA exclusions in the U.S., breach of data found in e.g. pension plans and health benefit plans, can be a special condition that is not covered.
- **Prior acts** - Since there may be a long time between time of breach and time of discovery, exclusions can limit the covered incidents originating from before policy inception and long tailed consequences.
- **The insured vs insured** - Such exclusion state that a claim made by one insured against another insured is not covered, however, there can be carve-backs for various reasons such as violation of privacy.

4.3 Clarifying loss

It is also useful to clarify what costs are covered for different types of cyber events. The data material from Advisen divides this into the following four categories, which we have detailed using definitions from Allianz [11]:

- **Response costs** - E.g. forensic investigations, identifying and preserving lost data, advice on legal and regulatory duties, notification costs according to legal and regulatory requirements, determining the extent of indemnification obligations in contracts with third party service providers, credit monitoring services and other remedial actions required after a loss of data, public relations expenses to handle negative publicity.
- **Economic loss** - E.g. loss of business income caused by a targeted attack, indemnity for stolen funds, indemnity for cyber extortion.
- **Litigated cases** - Defense costs and damages for which the insured is liable.
- **Fines and penalties** - Monetary fines and penalties levied by regulators arising from a loss of data.

Considering these categories, the Advisen data show that *response costs* has the highest average cost, while *economic loss* has the lowest, averaging about one third of response costs. Any organisation should during the negotiation get a clear definition about what kind of costs are covered for different types of incidents, and check these caps.

5 Conclusion

Cyber insurance has gained less ground in Europe than in the U.S., but with emerging laws and regulations, the prospect of considerable fines for security breaches is pushing many organisations into this market. What remains to see is: Can these organisations properly navigate through the still immature and obscured maze of cyber insurance products, or will they be easy prey for insurance companies offering policies that will not be worth much in the case of cyber events?

We have shown that the demand side struggles with several uncertainty factors when it comes to cyber insurance, and this has hindered the confidence in the product and market adoption process. Our qualitative interview study was based in Norway, but we believe that the same observations are found wherever regulations have not been a strong driving force yet. With an expected increase in this market, there is a need for better guidance in the consideration processes, as well as clearly defined and understandable terms and conditions for the product. This especially includes the identification of security gaps within the organisation, and coverage gaps, exclusions and loss types for the cyber insurance policy.

It was also found during the interview studies, that even for organisations that did not end up buying an insurance, there were still positive effects from the consideration process, since it brought attention and awareness of cyber security to the management level and across the organisation.

Acknowledgments. This research has been performed as part of the inSecurance project funded by SINTEF Digital. We would like to thank the representatives from all the organisations that participated in the interviews for sharing their experiences with us, and discussions with representatives from brokers and insurance companies. A final gratitude to Professor Guttorm Sindre at NTNU for feedback and comments.

References

1. Association of British Insurers: Making sense of cyber insurance: A guide for SMEs. Tech. rep., ABO (2016)
2. Bandyopadhyay, T.: Organizational adoption of cyber insurance instruments in it security risk management: a modeling approach. Proceedings. Paper 5 (2012)
3. 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)
4. Bentz, T.: Negotiating key cyber exclusions. insuranceday (2015), https://www.insuranceday.com/news_analysis/legal_focus/negotiating-key-cyber-exclusions.htm
5. Böhme, R., Schwartz, G.: Modeling cyber-insurance: Towards a unifying framework. In: Workshop on the Economics in Information Security (WEIS) (2012)
6. Cambridge Centre for Risk Studies: Managing cyber insurance accumulation risk. Tech. rep., University of Cambridge (2016)

7. Cohn, C., Barlyn, S.: European, asian companies short on cyber insurance before ransomware attack (2017), http://www.reuters.com/article/us-cyber-attack-insurance-idUSKCN18B00H
8. CRIF: Cyber insurance and the terrorism exclusion... (2014), http://www.cyberriskinsuranceforum.com/content/cyber-insurance-and-terrorism-exclusion
9. DG Justice and Consumers: Reform of eu data protection rules (2016), http://ec.europa.eu/justice/data-protection/reform/index_en.htm
10. Digital Single Market: Digital scoreboard (2016), https://ec.europa.eu/digital-single-market/digital-scoreboard
11. Dobie, G., Collins, S.: A Guide to cyber Risk - Managing the Impact of Increasing Interconnectivity. Tech. rep., Allianz (2015), http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf
12. ENISA, Robinson, N.: Incentives and barriers of the cyber insurance market in europe. Report (June 28th 2012), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport
13. Gordon, L.A., Loeb, M.P., Sohail, T.: A framework for using insurance for cyber-risk management. Communications of the ACM 46(3), 81–85 (2003)
14. Hiscox: The hiscox cyber readiness report (2017), https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf
15. Hurtaud, S., Flamand, T., Vaissire, L.d.l., Hounka, A.: Cyber insurance as one element of the cyber risk management strategy (February 2015), https://www2.deloitte.com/lu/en/pages/risk/articles/cyber-insurance-element-cyber-risk-management-strategy.html
16. Lloyd's, Cambridge Centre for Risk Studies: Lloyds City Risk Index 2015-2025 (2015), hhttp://www.lloyds.com/cityriskindex/
17. Maude, F.: The role of insurance in managing and mitigating the riske (2015), https://www.marsh.com/uk/insights/research/uk-cyber-security-role-of-insurance-in-managing-mitigating-risk.html
18. Meland, P.H., Tøndel, I.A., Solhaug, B.: Mitigating risk with cyberinsurance. IEEE Security & Privacy 13(6), 38–43 (2015)
19. Nikolaeva, M., Rivet, M.: French central bank chief urges insurers to step up cyber risk coverage (2017), http://www.reuters.com/article/us-france-insurance-idUSKBN1591Q9
20. Pain, L.D., Anchen, J., Bundt, M., Durand, E., Schmitt, M.: Cyber: In search of resilience in an interconnected world (2016), http://www.swissre.com/library/archive/Demand_for_cyber_insurance_on_the_rise_joint_Swiss_Re_IBM_study_shows.html
21. Ponemon: Managing cyber security as a business risk: Cyber insurance in the digital age. Report, Ponemon Institute (August 2013), http://www.ponemon.org/blog/managing-cyber-security-as-a-business-risk-cyber-insurance-in-the-digital-age
22. Protection, N., of Homeland Security, P.D.D.: Cyber risk culture roundtable readout report. Report (2013)
23. Protection, N., of Homeland Security, P.D.U.D.: Cybersecurity insurance workshop readout report. Report (2012)
24. Romanosky, S.: Examining the costs and causes of cyber incidents. Journal of Cybersecurity (2016)

25. Siemens, R., Beck, D.: How to buy cyber insurance. Risk Management 59(8), 40 (2012)
26. Svanemyr, S.: Kontantene forsvinner i butikkene (Norwegian) (2016), https://tinyurl.com/j7qaqe9
27. Swiss Re Institute: Cyber: getting to grips with a complex risk. Tech. rep., Swiss Re (2017), http://www.swissre.com/library/sigma_01_2017_en.html
28. World Economic Forum: The global risks report 2016, 11th edition (2016), http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf