Does Insurance Have a Future in Governing Cybersecurity?

Article *in* IEEE Security and Privacy Magazine · September 2019

DOI: 10.1109/MSEC.2019.2935702

2 authors, including:

Daniel W Woods
The University of Edinburgh
43 PUBLICATIONS **374** CITATIONS

SEE PROFILE

Does insurance have a future in governing cybersecurity?

Daniel W. Woods and Tyler Moore

Accepted Article

Daniel W. Woods is with the Department of Computer Science, University of Oxford, 15 Parks Rd, Oxford OX1 3QD, UK.
E-mail: daniel.woods@cs.ox.ac.uk.

Tyler Moore is with the Tandy School of Computer Science, the University of Tulsa, 800 S Tucker Dr, Tulsa, OK 74104, USA.
E-mail: tyler-moore@utulsa.edu.

Abstract—Cyber insurance could achieve public policy goals for cybersecurity with private-sector means. Insurers assess organizational security postures, prescribe security procedures and controls, and provide post-incident services. We evaluate how such mechanisms impact security, identify market dynamics restricting their effectiveness, and sketch out possible futures for cyber insurance as governance.

Index Terms—cybersecurity governance, private governance, cyber insurance, technology policy

1 Introduction

Despite grabbing policymakers' attention, cybersecurity has seen very few policy measures adopted. Efforts to spur investments in cybersecurity have been modest and diffuse. Ex-ante obligations tend to be industry specific and avoid prescribing technical controls in favour of specifying organisational processes that must be followed [1]. Organisations setting security budgets and deciding how much and where they should be spent must look beyond regulation.

Private governance influences how responsibilities and liabilities are aligned for organisations. For our purposes this consists of non-governmental entities creating rules and enforcement mechanisms that influence security decisions. For example, the Payment Card Industry Security Standards Council defines a standard for how merchants manage credit card data. This includes annual validation of compliance with the standard and fines for non-compliance resulting in lost data. Enforcement power is derived from controlling access to payment card networks. Merchants must either accept the standard or ask their customers to pay by other means. The resulting PCI-DSS standard is remarkably prescriptive in terms of how payment card data is handled, especially when compared with most public regulations.

The insurance industry provides another model of private governance. Ericson et al. [2] analyse how insurers attempt to control policyholder decisions to reduce ``moral risk'' in which policyholders act recklessly. Insurance contracts define rules to be followed, insureds are assessed before the contract is signed, premiums rise and fall depending on insured characteristics and behaviour, and claims-generating incidents are investigated. Although there is skepticism regarding the effectiveness, insurers can influence policyholder behaviour up to the point that switching to another provider or operating without insurance is preferable. Such processes occurring ``beyond the state'' [2] tie into a liberal theory of governance that de-emphasises state responsibility.

Given the limits of public policy measures thus far, enthusiasm for insurance as a form of cybersecurity governance is growing. Public institutions in the EU and the US have published reports exploring how they can support the cyber insurance industry resulting in increased security levels [3]. The impact will increase as more organisations purchase policies. Allianz, for example, predicts the cyber insurance market will grow to $20 billion by 2025, as identified in [4].

Insurers face incentives to put mechanisms of control in place to reduce cyber losses. Scholars predict the industry will increase security levels by offering premium discounts for more secure infrastructure [5]. Talesh suggests insurers focus on reducing losses post-incident by acting as the self-styled ``quarter backs of data breach response'' [6]. These claims about cyber insurance are based on intuition and self-reporting respectively. Establishing whether and how these mechanisms occur is necessary, especially given that policymakers are considering costly interventions to support the market [3]. Government acting as the (cyber) insurer of last resorts is frequently proposed, for example.

This article explores how cyber insurance influences security decisions. We first evaluate whether predictions about the governance role of cyber insurance are borne out in reality. We then identify how market dynamics and product norms limit the potential governance role of

cyber insurance. Finally, we reflect on trends in both cyber insurance and broader operational risk by posing open questions about future paths involving cyber insurance's role and evolution in the future.

2 Cyber insurance as governance

Cyber insurance was predicted to impact security behaviour before any evidence was collected. In 2001, Schneier [5] envisaged a world where every organisation purchases network security insurance with discounts offered for security enhancing decisions like replacing an ``insecure Windows system'' with a more ``secure version of Linux''. The optimistic essay ends by suggesting ``good security [will be] rewarded in the marketplace'' as insurers recognise ``computer security *snake-oil* peddlers'' [5].

A 2008 report [7] echoed Schneier's vision of premium discounts as incentives, while also suggesting discounts could be used as security metrics. Security investments offering a bigger discount would be viewed as more effective. These discounts would be based on knowledge generated by aggregating claims data or even commissioning primary research. Despite the report being commissioned by a policy making institution, the authors offered a *wait-and-see* conclusion regarding possible policy measures in support of the market.

While these arguments are intuitively appealing, a review of cyber insurance in 2010 revealed that "positive expectations about cyber-insurance have not been analyzed rigorously" [8]. Informal conjectures claimed the insurers would impact security levels or generate knowledge without any corresponding parameters or model features. If this was a criticism of theoretical research, their observations of empirical research went even further by stating ``we are not aware of any quantitative empirical work on cyber-insurance markets''

Yet policymakers in the United States and the European Union latched onto the idea that insurers can incentivise better risk management. Reports released from 2012 onward by public institutions in the US and the EU suggest insurance contracts will contain ``prescribed security controls and procedures'' [3] that the policyholder must implement for coverage to be valid. All of the private governance mechanisms covered in this section were discussed at some point. Yet these reports were largely based on individual views of the market not empirical findings.

Talesh [6] explored the topic by collecting evidence from industry conferences, educational webinars, and marketing documents. This self-reporting by insurers supports the conclusion that ``insurer-sponsored help is greatly appreciated by organizations''. The article concedes that suggesting this leads to a ``net benefit'' (p.437) is premature, especially given that Talesh admits ``the value of these insurer-sponsored risk management services'' remains an open question.

We collect together a list of mechanisms by which insurers are claimed to affect cybersecurity:
C1 Assess Security Levels: "measure the organization's practices and make sure they are consistent with the prevailing security standards'" [6];
C2 Incentives for Investment: choice of systems and security controls ``will be strongly influenced'' [5] by premium discounts'
C3 Create Security Obligations: contracts will contain ``prescribed security controls and procedures'' [3];
C4 Access to Response Services: provide ``a menu of services that an organization can quickly access in the event of a data breach'' [6];
C5 Generate Knowledge: aggregate claims information and conduct primary research to develop an understanding of cyber risk [7].

Before policymakers endorse insurance as an effective form of governance, we should evaluate these claims by collecting empirical evidence.

3 The evidence so far

We conducted nine interviews with underwriters operating from the Lloyd's of London market, which sells insurance to international clients. We also consider the findings of several empirical studies. Romanosky et al. [4] analysed 235 regulatory filings regarding cyber insurance policy terms, application forms and pricing algorithms. Woods et al. [9] mapped the security controls found in 24 cyber insurance application forms to two popular information security standards. Franke [10] conducted interviews with 15 insurance professionals based in Sweden. Axon et al. [15] analyse 70 cyber insurance claims.

Application forms collect information relevant to information security [4, 9] confirming that insurers assess security (**C1**). Which aspects of security are measured is a more interesting question. A study of 44 applications forms found only ``only very rudimentary information is collected'' about technical infrastructure [4]. Further, many forms do not collect any information about entire sections of popular information security standards [9].

Often these forms are not even filled out because brokers push underwriters to assess larger clients based on *market meetings*. Multiple underwriters ask representatives from the insured questions about IT architecture and security measures over a phone call. Interviewees reported questions going unanswered. One suggested insurance can be bought without naming ``who your dependencies are'', undermining the insurer's ability to monitor vendors.

The Swedish interviews [10] suggest implementing security controls and procedures leads to premium discounts (**C2**). Although some Swedish insurers do not ``actually put this into practice'' [10], suggesting discounts ``suit bigger clients better''. Our UK respondents offered discounts based on a holistic view of an applicant's security but cannot quantify the effect of a control in isolation.

One interviewee suggested accreditation to standards does not lead to a ``massive discount'', while another said ``it is not like a 10% discount if you take good logs''. A separate interviewee suggested discounts for ``IT security'' were coming down because ``more of the issues are coming out of procedure''. Romanosky et al. [4] found that 45% of pricing algorithms filed with US regulators did not even consider information security.

Organisations face little additional incentive to comply with the security policy once a policy has been purchased (**C3**). The most commonly observed exclusions were ``not necessarily directly related to the cyber realm'' [4]. The exception proves the rule in Columbia Casualty Company v. Cottage Health System, in which an insurer denied coverage because the Insured used ``factory default system configurations'' and systems in which ``security patches were no longer even available, much less implemented'', despite representing otherwise in the application. This was the first such case and it was widely held that these terms should have been negotiated out of the contract, suggesting insurers can not punish policyholders for flaunting basic security procedures.

Insurers are more likely to exclude types of losses or causes of incidents. Famously, one insurer excluded coverage for the NotPetya attack claiming it constituted an act of war, which had already been identified as a potential issue in [3]. Although this legal case relates to a property insurance policy, cyber insurance policies contain similar exclusions but none have been enforced thus far. Romanosky et al. [4] observe that ``almost half'' of the policies in their sample exclude losses related to extortion or ransom. Many of the analysed policies were written before ransomware become widely used by cyber-criminals. Many of the interviewees have adapted their policies to reflect this.

All of our interviewees supported the view that post-incident services (**C4**) reduce losses. Axon et al. [15] show that “lawyer services” and “breach counsel” are the most common costs in cyber insurance claims, suggesting insurers do provide these services. There is, however, a potential conflict of interest when the insurer chooses the provider. This forces a choice between acting to minimise the client's losses or the insurer's indemnity payment. For example, a public statement might be seen favourably by regulators when considering the size of a fine, which the insurer would indemnify, while also causing reputation damage, which the insurer would not indemnify.

The preceding evidence could result from an immature market. Insurers may first need to generate knowledge and understand the market (**C5**). One insurer discontinued a subsidiary conducting loss research into information risks in the early 2000s [7], and we are not aware of any similar insurance industry-sponsored R&D outfits. Increasing understanding by aggregating claims data is limited by inconsistent data collection in an unstandardised format [3]. However, individual underwriters we interviewed were admirably committed to learning about information security via formal courses, news reports, academic articles and other such resources. This focus on education is extended to clients. One interviewee's firm offered an online cybersecurity awareness platform and monitored how often the insured party used it, which was also a ``good way to to gauge culture''.

Unfortunately this does not seem to be translating into innovation in policies or underwriting methods. Studying policies from 2007 to 2017 did not reveal ``any substantial changes in policy length, style, or composition over time'' [4]. Only 15% of 395 insurance professionals responding to the 2017 Advisen cyber insurance market trends survey reported that "systemic events such as the Dyn DDoS or the WannaCry Ransomware event'' had a moderate or significant impact on underwriting, with 45% reporting no impact whatsoever.

The evidence suggests today's cyber insurance market is not fully delivering on its predicted governance functions, with security obligations in contracts particularly lacking. The next section explores why this is the case.

4 WHAT IS PREVENTING GOVERNANCE?

The lack of focus on security posture in the risk assessment could be explained by a phenomenon observed in [3]. Brokers direct applicants towards insurers with the least stringent application process, creating a race-to-the-bottom in risk assessment. Many respondents want the market to *harden*---move away from an over-supply of insurance---so that insurers can ``start asking tougher questions and start demanding things of the client''. Woods et al. [11] collect evidence suggesting that cyber insurance premiums in the Californian admitted market are falling, with latest data point in 2019, suggesting the over-supply of insurance continues.

The Payment Card Industry Security Standards Council has sidestepped this problem by jointly developing a standard and ensuring providers do not deviate from enforcement. Such an approach by insurance carriers would likely violate competition laws.

We are yet to see evidence insurers can directly improve security via premium discounts. The cost of most security controls dwarfs the benefit in terms of reduced premium, which suggests discounts only provide incentives to invest at the margin. Furthermore, insurers do not provide discounts for individual controls but instead for a holistic view of security. Insurers offering discounts for security controls already in place is different to offering discounts as an incentive to implement security. The latter is like suggesting cinemas encourage pursuit of further education by offering discount ticket prices to students.

It is natural to ask why insurers would offer greater incentives to invest than already exist. A rational insured would already have a cost-effective security control in

place. This is because security controls accrue more benefit to the insured than the insurer, given that insurers only cover a subset of the potential losses. A counterargument focuses on interdependent security [8] in which security controls provide security for other policyholders beyond the one who makes the investment. This means the insurer is uniquely placed to internalise the positive externality, and would do so by incentivising security. It is an empirical question whether the benefits from interdependent security will overpower the insurer covering a subset of the potential loss. It is worth noting that none of our interviewees mentioned interdependent security, as it is a concept more associated with academic discussions.

Exclusions (such as withdrawing coverage if security patches are not applied) are mysteriously absent in insurance policies. One explanation could be broker commission, which tends to be a percentage of the premium. This incentivises negotiating for broader coverage with less security obligations rather than a lower price with more security obligations. Another explanation could be that insurers recognise that the implementation of security controls is imperfect, and they want to assure their clients that they will pay out claims in the event of a breach.

Once again, the comparison to PCI DSS is instructive: in nearly all high-profile thefts of payment card data, investigators have retroactively found the affected firms to be non-compliant with PCI rules and therefore subject to penalties. This has dulled the incentive to spend the resources to become compliant in the first place. And insurers do not wield nearly as powerful of a stick as the PCI council does (suspending acceptance of credit card payments). It therefore seems reasonable to offer broader coverage in order to attract customers in a competitive marketplace.

In other words, customer relations matter a lot. Cuthbert Heath famously offered to ``pay all claims in full'' following the 1906 San Francisco earthquake [13] without auditing the claims. Insurers may pay claims from organisations not following security procedures in order to maintain trust in the product, which is essentially a promise to pay out. Yet the lack of security obligations could lead to moral hazard polluting risk pools, in which bad risks joining the risk pool increases expected losses, to the cost of customers following such procedures.

Post-breach services are the success story of cyber insurance. Insurers provide these services because they reduce incident costs that insurers would have to otherwise indemnify. Whereas, risk mitigation leads to benefits in terms of attacks (and therefore claims) avoided, which is harder to observe. Monitoring risk mitigation measures is costly and the potential for misconfiguration undermining efficacy is great. Alternatively, security vendors have not been able to demonstrate that their products reduce losses, unlike say fire doors in property insurance.

The lack of change in policy composition over time could result from innovation not tracked by the regulatory filings analysed in [4]. Underwriters pursuing further education and independent research leads to better decisions without formal documentation. It is also possible that requiring insurers to file when they update policy wording or prices is dampening innovation.

We next consider what might change in the future..

5 Will cyber insurance even exist in ten years?

A fundamental question for cyber insurance is whether it will even exist in the future as a distinct offering. At present, a considerable proportion of traditional policies do not affirmatively include or exclude cyber coverage. The resulting ambiguity is known as "silent cyber" [3]. The industry is currently moving to remove this ambiguity using exclusions.

Multiple participants believed cyber risks will be affirmatively included in traditional lines. This future sees cyber attacks as a peril not unlike fire or workplace accidents. Traditional losses caused by cyber attacks or cyber liability assigned by courts would be realised as in the non-cyber equivalents. This would mirror environmental liability insurance which received much attention as standalone cover in the 1980s but is not widely bought.

A contradictory future sees cyber insurance emerge as a standalone product that every organisation buys. It would cover all losses emerging from cyber attacks including ransom demands, liability and business interruption. Differentiating risks like this helps insurers address problems like adverse selection and moral hazard. Cybersecurity expertise could additionally be concentrated with insurance professionals involved in selling standalone cyber insurance.

If cyber insurance is absorbed into traditional lines, the private governance effects will be more diffuse. It is an empirical question whether this is more effective in changing security practices. On the one hand, individual underwriters will have less specialised expertise in conducting in-depth cyber risk assessments or issuing security advice. On the other hand, it might see cyber risk integrated into organisational risk management on an equal footing with other risks, potentially leading to more resources allocated to cybersecurity.

In large part, this debate results from the lack of clarity in the term *cyber* insurance. Böhme et al. [12] suggest differentiating coverage by the type of asset *and* the means of risk arrival. Cyber-threat insurance, which covers physical losses causes by logical attack, could be absorbed into traditional lines. Offering coverage for information assets may be more difficult. It is worth noting the industry response to "silent cyber" has generally been to exclude losses caused by logical attack and offer coverage under standalone cyber insurance coverage [3].

6 Can insurance improve cyber hygiene?

Another question concerns the depth of risk assessment. This could shift if policyholders with stronger security postures recognise that the lack of rigorous risk assessment is polluting risk pools. Perversely, buyers with a strong security posture relative to other buyers should seek out insurers conducting in-depth risk assessments. The time cost of communicating information about security posture results in better risk selection and fewer claims for the insurer to pay, which *should* translate into lower premiums. Brokers are well placed to lead this change as they understand which insurers conduct rigorous assessments. It may not be in brokers' self-interest because communicating this information requires more of the broker's time, which is not rewarded as they are paid by commission.

Insurers refusing coverage for organisations who flaunt basic security procedures (like using default system configurations) should be applauded for preventing moral hazard from polluting risk pools. Policyholders who follow basic procedures must cross-subside otherwise. However, there is a fine line between requiring a basic security level from insureds and withdrawing coverage to avoid paying out on claims. Some entity should monitor this, whether that be a regulator, broker or a consumer group.

The presence of security obligations in contracts touches on the general lack of standardised policy wording. Industry bodies or regulators could force more standard contracts [3]. Consumers would benefit from standard policies allowing comparison between products offered by insurers. However, insurers would be restricted in their ability to innovate in response to the dynamics of cybercrime.

Brokers are the primary beneficiaries of the current non-standard market. They earn commission by reducing transaction costs for organisations looking to buy insurance. Diversity of products increases the value of specialising in assessing and negotiating the terms and price of cyber insurance policies. The race-to-the-bottom effects are likely to remain present while insurers rely on intermediaries to sell cyber insurance products, which undermines insurance as governance.

7 Will an actuarial science of cybersecurity emerge?

Power [14] charts the rise of risk management and its impact on organisational life. The concept of operational risk, to which cyber risk contributes, emerged from the financial sector. Power suggests the ``actuarial base for operational risk insurance must be suspect'' due to the low frequency of events. Turning to how the actuarial base might be built, historic claims data is sought after.

The majority of the market is open to sharing while a few insurers see claims data as their competitive advantage [3]. Unfortunately, these insurers also tend to hold most of the data. The value of claims data could tilt the market towards a natural monopoly which can only support a few dominant firms. The next best thing is databases that aggregate all publicly reported incidents. These will continue to grow over time but are limited by reporting biases; incidents related to availability or integrity, which tend not to compromise personal data, do not fall under mandatory reporting laws.

The actuarial base is further undermined by a tension between long-term analytics and short-term expediency. A participant suggested proposal forms provide standardised data collection that could lead to an ``analytic database'', but large companies are moving ``more towards meetings and calls''. This trend could see cyber insurance descend into an art based on the ad-hoc judgement of underwriters. Many participants were optimistic about ``security score card science'' providing an objective basis for analytics. This involves collecting data by scanning externally facing nodes on the applicant's network to provide a single score like a credit rating.

Power's [14] account of reputation risk provides a cautionary tale for standardised risk assessment, such as security scores. External agencies created evaluation metrics which cannot be challenged by the organisation under evaluation. The criteria of these metrics were internalised over time, displacing values linked to the organisation's particular context. This may result in a sub-optimal use of resources by emphasising externally observable controls over more effective ones.

Sub-optimal allocation of resources might also result from ``micro-politics'' [14] within the organisation, empowered by cyber insurance. Departments like IT and human resources compete for responsibility and resources regarding risk management. If the application forms value legal compliance over technical infrastructure, as seems to be the case [4, 9], the legal department may use this to justify taking responsibility away from the IT department. Insurers focusing on process could result from the streetlight effect rather than what is optimal for the organisation.

Relationships between insurers and security service providers is troubling. Participants revealed that they received advice in exchange for recommending the vendor to their clients, sometimes even requiring insureds use that vendor's services or products. Beyond the anti-competitive aspects, we should question the role of commercial interest in providing this advice. It could be warping the underwriters view of what constitutes an effective security investment. One might also question the social desirability of the most common claims costs [3] going towards professional services rather than restitution for victims, who are often customers with little control over their data.

8 How to deal with the potential for cyber catastrophe?

The potential for correlated cyber losses is intimately

linked to how claims costs arise. Axon et al. [15] describe evidence suggesting that data breaches, ransomware and non-compliance with legislation are the most common triggers of cyber insurance claims. Data breaches rarely correlate across companies and costs assigned by courts are bounded by the judge's sense of proportionality, although insurers have fell victim to political judgments assigning costs to those deemed to have the deepest pockets in the past [13].

Ransomware incidents are different because many claims can result from the same underlying cause, as evidenced by the NotPetya attack. Incidents occurring independently, such as data breaches, can be absorbed by risk pools. However, correlated incidents pose an existential threat to the risk pool. The increasing prevalence of ransomware claims and the increased solvency risk may force insurers, possibly led by re-insurers, to influence cybersecurity levels in a way that we have not seen thus far. But we should be cautious given the number of false dawns seen so far.

Anxiety about aggregated or correlated losses will not abate until network complexity is reduced. Doing so would fundamentally reshape modern economies. Insurers instead try to track service providers as a point of correlated risk accumulation. If the market began to harden, they might be able to select or incentivise insureds to create more diversity and resilience.

Alternatively, the industry might move towards excluding coverage for systemic attacks. Poor communication in doing so undermines consumer trust. Criticisms were leveled following the NotPetya attack because the threshold for cyber war is ambiguous. Many of these criticisms were unfair given the policy in question was not sold as cyber insurance. Nevertheless, court battles are an expensive way to clarify expectations.

Insurers might instead lobby the government to become the re-insurer of last resorts. There are precedents in flood and terrorism insurance and many different forms this can take [13]. Proponents suggest these losses result from states failing to protect companies from other nation state attacks. Detractors ask why tax payers should cover the tail risk of private companies when they fail to comply with basic security procedures, such as patching the vulnerability behind the NotPetya attack.

Recalling why governments provide a backstop for flood and terrorism coverage is important in evaluating this policy measure. Reinsurers began excluding terrorism related losses following events in the US and the UK leading to re-insurers withdrawing coverage [13]. It was argued insurers would not offer policies to consumers unless a government backstop was provided. In contrast, policy reports have identified a lack of demand in the cyber insurance market [3], which cannot be solved by supply side measures like government backstops. This policy measure should be shelved until an under-supply of cyber insurance is identified.

9 Conclusion

Policy makers have long held high hopes for cyber insurance as a tool for improving security. Unfortunately, the available evidence so far should give policymakers pause. Cyber insurance appears to be a weak form of governance at present. Insurers writing cyber insurance focus more on organisational procedures than technical controls, rarely include basic security procedures in contracts, and offer discounts that only offer a marginal incentive to invest in security. However, the cost of external response services is covered, which suggests insurers believe ex-post responses to be more effective than ex-ante mitigation. (Alternatively, they can more easily translate the costs associated with ex-post responses into manageable claims.)

The private governance role of cyber insurance is limited by market dynamics. Competitive pressures drive a race-to-the-bottom in risk assessment standards and prevent insurers including security procedures in contracts. Policy interventions, such as minimum risk assessment standards, could solve this collective action problem. Policyholders and brokers could also drive this change by looking to insurers who conduct rigorous assessments. Doing otherwise ensures adverse selection and moral hazard will increase costs for firms with responsible security postures.

Moving toward standardised risk assessment via proposal forms or external scans supports the actuarial base in the long-term. But there is a danger policyholders will succumb to Goodhart's law by internalising these metrics and optimising the metric rather than minimising risk. This is particularly likely given these assessments are constructed by private actors with their own incentives. Search-light effects may drive the scores towards being based on what can be measured, not what is important.

Systemic risk has a number of possible futures. Organisations may have to accept liability as insurers exclude the risk. Governments might step in to offer re-insurance, though we caution against doing so until an under-supply of cyber insurance is observed. Or insurers might show leadership in encouraging diversity in technology and service provision to reduce systemic risk.

ACKNOWLEDGMENT

The authors wish to thank Rainer Böhme and the anonymous reviewers for providing constructive feedback. Thanks also go to participants at the Lorentz Center's workshop "Cyber Insurance and its Contribution to Cyber Risk Mitigation" for many interesting ideas about the role of brokers. The authors' collaboration was made possible by a Fulbright Cybersecurity Scholar Award.

REFERENCES

[1] Tyler Moore. The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection, 3(3-4):103–117, 2010.

[2] Richard Victor Ericson, Aaron Doyle, and Dean Barry. Insurance as governance. University of Toronto Press, 2003.

[3] Daniel W Woods and Andrew C. Simpson. Policy measures and cyber insurance: A framework. Journal of Cyber Policy, 2(2):209–226, 2017.

[4] Sasha Romanosky, Lillian Ablon, Therese Jones, and Andreas Kuehn. Content analysis of cyber insurance policies: how do carriers price cyber risk? Journal of Cybersecurity, 5(1), 02 2019.

[5] Bruce Schneier. Insurance and the computer industry. *Communications of the ACM*, 44(3):114–114, 2001.

[6] Shauhin A Talesh. Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry*, 43(2):417–440, 2018.

[7] Ross Anderson, Rainer Böhme, Richard Clayton, and Tyler Moore. Security economics and the internal market. Report to the European Network and Information Security Agency, 2008.

[8] Rainer Böhme and Galina Schwartz. Modeling cyber-insurance: Towards a unifying framework. In *Proceedings of The 9th Workshop on the Economics of Information Security (WEIS 2010)*, 2010.

[9] Daniel W Woods, Ioannis Agrafiotis, Jason RC Nurse, and Sadie Creese. Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications*, 8(1):8, 2017.

[10] Ulrik Franke. The cyber insurance market in Sweden. *Computers & Security*, 68:130–144, 2017.

[11] Daniel W Woods, Tyler Moore, and Andrew C Simpson. The county fair cyber loss distribution: Drawing inference from insurance prices. In *Proceedings of The 18th Workshop on the Economics of Information Security (WEIS 2019)*, 2019.

[12] Rainer Böhme, Stefan Laube, Markus Riek. A Fundamental Approach to Cyber Risk Analysis. *Variance* 12:2, 2019, pp. 161-185

[13] Rob Thoyts. Insurance theory and practice. Routledge, 2010.

[14] Michael Power. Organized uncertainty: Designing a world of risk management. Oxford University Press on Demand, 2007.

[15] Louise Axon., Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, and Sadie Creese. Analysing cyber-insurance claims to design harm-propagation trees. In 2019 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019.