Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: http://www.tandfonline.com/loi/rcyb20

Policy measures and cyber insurance: a framework

Daniel Woods & Andrew Simpson

To cite this article: Daniel Woods & Andrew Simpson (2017) Policy measures and cyber insurance: a framework, Journal of Cyber Policy, 2:2, 209-226, DOI: 10.1080/23738871.2017.1360927

To link to this article: http://dx.doi.org/10.1080/23738871.2017.1360927

Published online: 03 Aug 2017.

JOURNAL OF CYBER POLICY, 2017
VOL. 2, NO. 2, 209–226
https://doi.org/10.1080/23738871.2017.1360927

Routledge
Taylor & Francis Group

Policy measures and cyber insurance: a framework

Daniel Woods and Andrew Simpson

Department of Computer Science, Mathematical Physical and Life Sciences Division, University of Oxford, Oxford, UK

ABSTRACT

The role of the insurance industry in driving improvements in cyber security has been identified as mutually beneficial for both insurers and policy-makers. To date, there has been no consideration of the roles governments and the insurance industry should pursue in support of this public–private partnership. This paper rectifies this omission and presents a framework to help underpin such a partnership, giving particular consideration to possible government interventions that might affect the cyber insurance market. We have undertaken a qualitative analysis of reports published by policy-making institutions and organisations working in the cyber insurance domain; we have also conducted interviews with cyber insurance professionals. Together, these constitute a stakeholder analysis upon which we build our framework. In addition, we present a research roadmap to demonstrate how the ideas described might be taken forward.

ARTICLE HISTORY
Received 3 June 2017
Revised 27 June 2017
Accepted 28 June 2017

KEYWORDS
Cyber insurance; cyber security; public–private partnership; policy measures; stakeholder analysis

1. Introduction

At the turn of the century, security specialist Schneier (2001) described a world in which the 'computer security industry will be run by the insurance industry'. In such a world, Schneier envisaged information security decisions being impacted by an insurer's checklist. However, these checklists commit the '4th deadly sin of information security' – not identifying the organisation-specific risks – as introduced by Von Solms and Von Solms (2004).

Schneier's vision was motivated (at least in part) by an analogy with property insurance where sprinkler systems are installed because 'building codes and insurance policies demand it'. The nascent cyber insurance industry's failure to deliver on initial growth predictions means that such a world is not yet a reality. However, the underlying principle that the insurance industry will improve information security management is fundamental to a public–private partnership for cyber insurance.

Policy-makers have been seriously considering the impact and viability of such a partnership since at least the 2003 Homeland Security Council,[1] at which Paul B. Kurtz argued that '[Offering cyber insurance policies] may be easier said than done [but] somehow it can be done'. Less than 10 years later, the US Department of Homeland Security (2012, 2013, 2014a, 2014b) convened a 'Cybersecurity Insurance Workshop' and a series of other round-

CONTACT Daniel Woods

tables and working groups. ENISA (2012, 2016) published an analysis of the barriers to a European cyber insurance market in 2012, with a follow-up report in 2016. In 2015, UK Cabinet Office (2015) published a policy paper entitled 'UK cyber security: the role of insurance'. These discussions illustrate the progression of the market from one security expert's vision to an issue worthy of the attention of governments.

Yet the diversity of interests leads to disparate analysis and discussion of the topic. While some collaboration has taken place, there is no forum that has successfully incorporated all of the global stakeholders, including insurance carriers, critical infrastructure owners, risk managers and owners within businesses, IT experts, academics and policy-makers. Consequently, much of this discussion is broken down into national and industry silos. Such a situation is untenable given that many of the insurers and policyholders operate internationally: a fragmented policy landscape could provide an additional barrier to the growth of the market.

The paper introduces a framework to understand the contributions from policy-makers and the insurance industry towards a cyber insurance public–private partnership. These contributions consist of government interventions and private sector initiatives that were identified in the aforementioned reports published in the U.S., the U.K. and the E.U. Our stakeholder analysis explores how the interests of policy-makers and the insurance industry align with the identified policy measures. Buyers of cyber insurance are considered out of scope. The framework provides the first consideration of how the different policy discussions interrelate and an understanding of where there is scope for coordination between stakeholders. In addition, we identify a series of prioritised top-down policy measures and present a research roadmap linking this framework to future work that could support a public–private partnership for cyber insurance.

The next section provides some background related to the insurance industry. The methodology used is then outlined in Section 3. In Section 4, we derive the themes and show the results of our stakeholder analysis. The framework is presented in Section 5, together with our research roadmap. We present conclusions in Section 6.

2. Background

We consider first, work that illuminates the business processes that are relevant to a public–private partnership for cyber insurance. Camillo (2017) outlined the 'surprisingly long history of cyber insurance' – in which the number of standalone cyber insurance providers has been growing since the turn of the millennium. Camillo identified the TJX hack in 2007, which resulted in over 45 million financial records compromised, as a turning point. Today the market offers a wide range of insurance products to enterprises of varying sizes. Camillo concludes by highlighting predictions that the market could grow to in excess of U.S.$20 billion by 2025.

Insurers offering products face the problem of *adverse selection*, where a firm may apply for cyber insurance in the knowledge that they are relatively more exposed to cyber risk. Kesan, Majuca, and Yurcik (2005) describe how this issue is addressed by extensive *ex-ante* assessment in order for an underwriter to classify the applicant into a given risk category and then set the insurance premium. The application process involves collecting information via self-assessed questionnaires (proposal forms), telephone interviews and

client presentations. Camillo (2017) explains how insurers become a 'de facto regulator' by establishing a minimum security level to gain cyber coverage.

Two methods of 'regulation' that are well founded in insurance law are *subjectivities* and *warranties*. In the context of cyber insurance, *subjectivities* could involve a policy being offered subject to a given security control being put in place. A *warranty* might make the insurance policy's validity dependent on implementing prescribed security controls and procedures. Warranties can address *moral hazard*, which involves a policyholder engaging in risky behaviour in the knowledge an insurance policy covers the consequences.

Moral hazard is also addressed by the ongoing relationship between the insurer and the policyholder. In the event of a cyber attack against the policyholder, insurers partner with external security professionals to offer services such as incident response or public relations management to limit damage to the company. In return, these security professionals offer cyber security advice to help the insurer better understand the risks that they cover. Additionally, the insurer may request a forensic investigation as part of the claims process. This would seek to establish the cause and extent of the loss before indemnifying the policyholder.

The assessment and claims procedures provide an opportunity for data collection, while the ongoing relationship enables information-sharing and guides security decisions. These interactions between the insurer and the policyholder inform some of the policy measures that could be part of a public–private partnership. Government intervention in the cyber insurance market is justified by previous failure of cyber insurance to deliver upon expectations. For example, Majuca, Yurcik, and Kesan (2006) highlight predictions that cyber insurance would be a U.S.$2.5 billion market by 2005; yet it has only reached that level in the past year.[2] To the best of our knowledge, there has been no academic work investigating the range of policy measures affecting the cyber insurance market.

3. Methodology

To align with pre-existing policy discussions, the framework's themes were established by studying a number of reports that consider challenges related to the cyber insurance market. Each theme contains a number of policy measures, which consist of government interventions and private initiatives. To understand the viability of each policy measure, we conducted a stakeholder analysis to establish the level of support.

3.1. Identifying themes and policy measures

We investigated published reports on cyber insurance from the US Department of Homeland Security (2012, 2013, 2014a, 2014b), the UK Cabinet Office (2015) and ENISA (2012, 2016). The U.S. is the largest market for cyber insurance and many of the leading insurance providers operate out of the U.S. The E.U. contains a large market for cyber insurance, and its policy decisions impact both Germany and the U.K., two significant markets. The U.K. was included because the British market exhibits 'a higher level of maturity' than the rest of the E.U., as described by ENISA (2016).

The U.S., the U.K. and the E.U. provided four, one and two reports, respectively. We are not aware of a comparable report published by the German Government; this may

Table 1. Details of the reports published on the cyber insurance market.

Code	Title	Author	Date
[EU1]	Incentives and barriers of the cyber insurance market in Europe	European Union Agency for Network and Information Security	June 2012
[EU2]	Cyber Insurance: Recent Advances, Good Practices and Challenges	European Union Agency for Network and Information Security	November 2016
[UK1]	UK cyber security: the role of insurance	UK Cabinet Office	March 2015
[US1]	Cybersecurity Insurance Workshop Readout Report	US Department of Homeland Security	November 2012
[US2]	Cyber Risk Culture Roundtable Readout Report	US Department of Homeland Security	May 2013
[US3]	Cyber Insurance Roundtable Readout Report	US Department of Homeland Security	February 2014
[US4]	Cyber Insurance Working Session Readout Report	US Department of Homeland Security	July 2014

be (in part) explained by a recent report on insurance in the U.S., the U.K. and Germany, which found that German firms were the least likely (when compared with firms from the U.S. and the U.K.) to have cyber insurance (30%).[3] The collection of reports contained in Table 1 outlines a number of policy measures, in addition to identifying challenges to an effective cyber insurance market. We reference the report from which the policy measure originated and every subsequent report mentioning it.

3.2. Stakeholder analysis and the resulting framework

The stakeholders consist of the departments responsible for considering cyber insurance policy in the U.S., the U.K. and the E.U., one organisation representing a coalition of insurers (Lloyd's of London), and a number of individual insurers based in the U.K. We did not include cyber insurance buyers as stakeholders because we assume that buyers are unlikely to be informed about the wider cyber insurance market. Further, their interests are generally represented by the policy-makers' responsibility for consumer protection. Cyber insurance buyers are out of the scope of this paper. However, further study of their interests is included as a priority area for further research in Section 5.3. The reports published by the U.S., the U.K. and the E.U. allowed us to capture the interests and priorities of each.

Lloyd's of London is a global market for insurance, with 41% of Lloyd's global premiums collected in the U.S.[4] The Lloyd's corporation regulates the Lloyd's market and manages the mutual fund; this is a unique arrangement (although other organisations representing a coalition of insurers do exist). The interests of Lloyd's were represented by the 2017 market oversight plan[5] and the Lloyd's cyber attack strategy[6] which we will refer to as [LL1] and [LL2], respectively.

We established contact with nine insurers through an insurance broker. These firms were chosen because they represent a range of different market strategies: targeting small businesses and large multinationals, and offering bespoke policies, and 'off-the-shelf' insurance products. All of our participants operate out of Lloyd's of London. We acknowledge that this could result in sample bias; however, there is no alternative specialist market in the U.K. The interests of each participant were established during semi-structured interviews, which allowed us to explore the views and issues raised in detail.

The resulting framework draws together the themes, the policy measures and the stakeholder analysis, with the themes providing the structure of the framework. For each

policy measure we provide an overview of how each of the stakeholder's interests relate to it, identifying where common interest can serve as the foundation for greater coordination.

4. Results

In this section, we discuss each theme in turn, discussing the range of policy measures affecting that theme and the stakeholder support for each.

We start by describing how we derived the themes from the published reports on cyber insurance, which are listed below:

(1) **Wider adoption** (Section 4.1)
(2) **Defining coverage** (Section 4.2)
(3) **Data collection** (Section 4.3)
(4) **Information sharing** (Section 4.4)
(5) **Best practice** (Section 4.5)
(6) **Catastrophic loss** (Section 4.6)

Initial policy discussions were often framed as aiding growth of the market. For example, [EU1] focuses on 'barriers to growth', while [UK1] focuses on the small size of the U.K. market. Policy initiatives related to this fall under the theme *Wider adoption* (Section 4.1). If the previous theme relates to the size of the market, then *Defining coverage* (Section 4.2) relates to the 'shape' of the market. [UK1] suggests that a 'lack of product consistency can lead to trust issues'. A participant in the DHS working group suggested that the variability in 'defining cyber incidents across international boundaries' would be a barrier to participation in a cyber data repository.

The next two themes relate to data. The first is how data is collected, under the theme *Data collection* (Section 4.3). [EU1] identifies the availability of 'robust actuarial data' as a major obstacle to cyber insurance, while [UK1] takes the view that 'historical data will only ever be partially relevant'. The second theme, *Information sharing* (Section 4.4), relates to how data are shared. All three reports agreed upon the utility of cyber insurance data for analytical purposes. For example, [US4] made creating a 'cyber data repository' one of the three priority objectives of the working group.

All of the reports suggest that cyber insurance will propagate best practice in information security management. For example, [US1] suggested a bigger market might 'incentivize firms to implement good cybersecurity practices'. Such efforts fall under the theme *Best Practice* (Section 4.5).

The most significant policy measure is a government acting as an insurer of last resorts in response to the challenge of *Catastrophic loss* (Section 4.6). [EU1] points to a 2010 conference reporting that a number of governments already intervene as a re-insurer of last resort. A participant in the DHS Workshop suggested that the U.S. Federal Government could provide re-insurance while the market matures and the actuarial data builds up. Similarly, [UK1] considers a variety of ways to facilitate a cyber re-insurance market. These six themes will be discussed in each of the following six subsections, before we draw them together into the framework in Section 5.

4.1. Wider adoption

4.1.1. Legislation creating a financial cost to cyber events [EU1, EU2, UK1, US1, US4]
4.1.2. Raise awareness about gaps in traditional insurance products [EU1, EU2, US1, UK1]
4.1.3. Governments to exercise their procurement power to support market development [EU1, UK1, US1]
4.1.4. Mandate insurance for organisations in certain industries [US4]

Legislation that assigns a financial cost to cyber events (4.1.1) is one factor in the demand for insurance; for instance, mandatory breach notification laws impose the cost of notifying affected parties upon the organisation suffering a data breach. [US1] suggests that the California Data Breach Laws of 2003, along with other pieces of legislation, had 'led to huge growth'. This is corroborated by [EU1], [UK1] and [EU2], which highlight the role of U.S. regulation in driving early demand for cyber insurance.

There is a hope that the forthcoming European Union General Data Protection Regulation (GDPR)[7] will drive demand for cyber insurance in Europe, as it includes a similar obligation on organisations operating in E.U. member states. However, one interviewee warned that the effects of the GDPR may not live up to expectations because 'fines and penalties are uninsurable', explaining that the financial cost must be insurable for such legislative acts to translate into increased demand for insurance.

The interviewee went on to describe that insurers in the U.S. are concerned with class-action lawsuits from customer groups, whereas in Europe it is the need to notify the Data Protection Authority (DPA) that is of concern. However, this could change: [EU1] suggested that an initial fact-finding exercise as to the scope for collective action or redress relating to cyber events would be useful. The specific legislative approach (U.S. collective action, as opposed to the European DPA model) will affect how insurers operate.

Governments could *raise awareness about gaps in traditional insurance products* (4.1.2). [US1], [EU1], [EU2] and [UK1] all identify a lack of understanding about existing insurance cover as a barrier to wider adoption of cyber insurance. It is often not clear who is responsible for addressing the problem: many interviewees thought this was the role of the broker, who has a direct relationship with the client; others felt that, as the problem was so universal, a stakeholder from outside the insurance industry would be more persuasive.

[UK1] and [US1] both suggest that governments could exercise *their procurement power to support market development* (4.1.3). [US1] suggests that organisations could be required to purchase cyber insurance coverage to win government contracts. Another option is to increase the demand by entering the market and encouraging government agencies to purchase cyber insurance; [UK1] suggests that this could take place for essential services and national critical infrastructure.

A stronger intervention could involve *making cyber insurance mandatory for organisations in certain industries* (4.1.4) – much like car insurance is mandatory in most countries. This could be limited to certain industries, firms of a certain size, or determined by some other characteristic. Mandatory insurance coverage would increase the regulatory burden on regulators who must ensure the availability and affordability of insurance coverage. For

example, a number of interviewees mentioned that they would not offer coverage to certain sectors, such as healthcare. Without further intervention, these sectors would face prohibitive costs to meet the mandatory insurance requirement. Any lever affecting the size of the market has linkages to other themes: a larger market will increase the amount of data collected (Section 4.3) and increase the risk of catastrophic loss (Section 4.6).

4.2. Defining coverage

4.2.1. Encourage the use of cyber exclusions in non-cyber policies [UK1, US1, US4]
4.2.2. Standardise wording of cyber insurance policies [EU2, US1]
4.2.3. Provide certification for acts of cyber war or terrorism [EU1]

The wording determines the underlying risks that cyber insurance covers. If wording varies across insurance policies, it is difficult to understand the extent of the aggregated risk; this problem is compounded by 'silent cover', which involves non-cyber policies providing unintended cover for cyber-related events.

[UK1] suggests that insurers could be *encouraged to use cyber exclusions in non-cyber policies* (4.2.1), such as the CL 380 clause common to policies for energy sector companies:

> In no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.

[US4] identified that some insurers' policies would exclude physical damage from cyber attacks, while others would not. In response to this problem, in [LL2] Lloyd's committed to 'encouraging the development and use of appropriate exclusions and sub-limits for cyber-attack'.

Positive clarification could move the market towards *standardised wording of cyber insurance policies* (4.2.2). For example, [US4] stated that variability in 'defining cyber incidents' could be a barrier to a cyber data repository, linking to the theme of data collection (Section 4.3). A push towards standardisation would likely be resisted by some insurers. For example, one interviewee stated:

> Awareness of risk is about tailoring coverage to fit your client's needs. There are so many people who will just sell the off-the-shelf products. Insurers must ensure that each policy is relevant to the client.

It should be noted that many large insurers are members of industry standards bodies, who recommend standardised policy wording and question sets.

Another interviewee thought that the exclusions related to cyber war and terrorism 'will be very very hard to prove'. Governments could *provide certification for acts of cyber war or terrorism* (4.2.3), akin to how the U.K. Government provides official confirmation that an act of terrorism has taken place for insurance purposes, as raised in [EU1]. Such efforts would be complicated by the difficulties faced in defining cyber war and the challenge of attributing a cyber attack to a particular actor.

4.3. Data collection

4.3.1. Standard data formats for assessment or claims process [UK1, US1, US4]
4.3.2. Minimum standards for data collection in assessment process [US2]
4.3.3. Government collects high-level data on the insurance market [EU1, US1]

The policy measures in this section all seek to improve the quality and volume of data that is collected. The claims process provides an opportunity to collect data with regards to how the event occurred, as part of the loss adjustment process. Governments could work with the insurance industry to define *standard data formats for the claims process* (4.3.1); [US1] discussed how the U.S. Federal Government could 'drive the development of metrics, requirements and standards'. This would tie into an existing Lloyd's initiative outlined in [LL2], which created two specific cyber risk codes in order to monitor claims data resulting from cyber attacks.

Similarly, the information collected during the application process differs according to the individual insurer. The qualitative nature of phone interviews and applicant presentations makes standardisation difficult. However, self-assessed questionnaires could provide a standard form of assessment. At present most insurers offer a questionnaire unique to their organisation. Lloyd's also provides a proposal form that insurers are free to use, which some of our interviewees take advantage of. However, other interviewees stated that they would refuse to accept another insurer's proposal form. This highlights opposition to a standard form for all insurers. A solution to this problem could be based on a *standard data format for the assessment process* (4.3.1) that every form must collect, beyond which an insurer would be free to ask whichever questions they liked.

[LL1] suggests that there will be little change to the 'prolonged soft market conditions' meaning that the over-supply of insurance capacity will continue, which can lead to less stringent underwriting. Interviewees were concerned that 'brokers are choosing the path of least resistance' and are approaching insurers with the least stringent assessment process; arguably, this creates a race-to-the-bottom in terms of collecting information related to security. [US2] reports that insurers are moving away from detailed assessments because of an increasingly competitive market. One response could be to establish *minimum standards for data collection in the assessment process* (4.3.2).

[EU1] suggested that the governments should collect high-level data on the insurance market (4.3.3) which would be beneficial. The report also commends pre-existing surveys, such as the U.K.'s annual Cyber Security Breaches Survey.[8] This task could complement or be supported by existing market data already collected, such as that collected by Lloyd's. In [US4], one broker suggested that the 'three existing lines of insurance with the most robust data and strongest predictability' entail mandatory coverage requirements.

A larger insurance market produces a greater volume of data and this links back to (1.4); the other options outlined in Section 4.2 could have a similar effect.

4.4. Information-sharing initiatives

4.4.1. Make data held by government agencies available [US1, US4]
4.4.2. Open up access to existing information-sharing initiatives [UK1]

4.4.3. Mandate other organisations to make data available [US1]
4.4.4. Government to create a cyber incident data repository [US1, US4]

The three policy-making institutions considered different information-sharing initiatives. [US4] made creating a 'cyber data repository' one of the three priority objectives. Meanwhile, [UK1] suggested that the insurance industry should be more involved in the cyber security information-sharing partnership (CISP), which enables government and industry to share information. Meanwhile, [EU2] recommended that cyber insurance customers should be more open about sharing data, with no mention of insurers or governments sharing information.

A suggested policy measure involves *governments mandating other organisations to make data available* (4.4.3); [US4] identified auditors for this as organisations are already mandated to share information with them. There is, though, opposition to information-sharing initiatives. For example, one participant in [US1] identified that 'top carriers don't want to share such information'. An interviewee commented that 'we're a market, not a cartel'; another raised concerns about remaining competitive while sharing information and issues related to anonymisation. Those insurers with a small amount of claims data were (perhaps understandably) far more enthusiastic about data being shared.

Mandatory disclosure laws support data availability. [US1] claimed that state-level data breach disclosure laws in the U.S. contribute to the available actuarial data about data breaches. The GDPR could have a similar effect in Europe; although it should be noted that DPAs already make available some data related to data breaches, such as the ICO in the U.K.[9]

Beyond the insurance industry, [US1] suggested that the U.S. Federal Government was in a unique position to *make data held by government agencies available* (4.4.1) but this was dismissed because of national security fears. This contradicts the response from one interviewee who revealed that he received briefings from the FBI while formally employed by a large U.S. insurer.

[UK1] suggested that policy-makers *could open up access to existing information-sharing initiatives* (4.4.2). The U.K. CISP approach mitigates one of the issues a participant raised in [US1], namely that access to existing information-sharing institutions 'is limited to sector members only'. An interviewee mentioned he already uses sector-specific Information Sharing and Analysis Center to understand the threat landscape for a particular industry, demonstrating the utility of insurers being granted access. Members of such schemes may be alarmed that their insurance premiums will be affected by the insurer joining the scheme. However, the principle of misrepresentation in insurance law means that the insured cannot withhold information that would otherwise affect the premium. Policy-makers should be aware of this tension so as not to disrupt the trust placed in information sharing initiatives.

Any combination of the policy measures outlined could support *governments in creating a cyber incident data repository* (4.4.4). [US4] reported stakeholder discussions about creating a cyber data repository. Incorporating data held by government agencies (4.1) and mandating other organisations to provide data (4.3) were both discussed. Integration with existing information-sharing initiatives was not discussed, but it is clearly a possibility. Data repositories will have to overcome the challenges of government agencies worried about national security concerns, the increased risk of data breach resulting from

managing the repository and organisations concerned that sharing data will lead to reputation damage (mitigated by mandatory breach disclosure laws).

4.5. Best practice

4.5.1. Government can define information security best practice [UK1, US1, US4]
4.5.2. Lead organisations to best practice through regulation [EU2, US4]
4.5.3. Clarify liability related to insurers giving security advice [EU1, Int, US4]

Policy-makers hope that the insurance industry can spread information security best practice. However, doing so requires identifying 'what' to spread and 'how' to spread it, and there is no consensus on what best practice looks like. [EU1] points to a number of information security standards published by member states as successful efforts to define best practice. [UK1] names each of Cyber Essentials, ISO 27001, NIST and 10 Steps to Cyber Security as possible sources of IT standards. At the DHS workshop, the National Institute of Standards and Technology (NIST) is suggested as a provider of IT security standards. Each suggests a standard by which a *government can define information security best practice* (4.5.1) that insurers can adopt; whether there is agreement on a specific standard will be addressed in Section 5.

[US1] identified avoiding government action as a driver towards companies adopting information security standards. The interaction between regulation and the insurance industry should be monitored, particularly with forthcoming regulation, such as the European Union Directive on security of network and information systems (NIS Directive),[10] which will be implemented by all E.U. member states. This suggests how policy-makers can *lead organisations to best practice through regulation* (4.5.2). However, [EU2] recommends against introducing mandatory security requirements that might undermine the cyber insurance market adoption rate.

Governments could *clarify liability related to insurers giving security advice* (4.5.3) as insurers are unsure as to their role. One interviewee worried that suggesting best practice might constitute professional advice. Another insurer who had seen 'well known companies that have absolutely terrible security' expressed a desire to distill best practice, but did not because of potential liability issues. [US4] identified 'current regulatory requirements that govern the provision of policy premium discounts' as a potential barrier to insurers requesting that security controls are implemented. All of these efforts should be conscious of a case study from [US3] depicting a policyholder resistant to additional regulation imposed by the insurer.

4.6. Catastrophic loss

4.6.1. Government to act as insurer of last resorts [EU1, UK1, US1]
4.6.2. Collect funds ex-ante [Pool Re] or ex-post [TRIA]
4.6.3. Membership optional [Pool Re] or mandatory [TRIA]
4.6.4. Premium priced according to underlying risk [Pool Re] or priced according to amount of insurance sold [TRIA]

4.6.5. Upper limit on the amount the scheme will cover [Sri Lanka]
4.6.6. Upper limit on the amount one insured can claim [OPIC model]

[EU1] identifies that nine *governments act as a re-insurer of last resorts* (4.6.1). The governments intervene with a variety of different mechanisms. We provide a brief outline of the structure of the U.S. and the U.K. approaches, with a view to understanding how the approaches differ.

In response to the Irish Republican Army's mainland bombing campaign in the U.K., Pool Re[11] was established to help ensure property insurance covered terrorist acts. Brice (1994) describes how Pool Re fund covers all claims resulting from terrorism above a pre-assigned amount, providing the insurer purchased Pool Re cover. The U.K. Government is liable for all losses exceeding 110% of the value of the fund. The fund comes from a combination of a levy on all household and motor policies, as well as the premiums charged to members of the fund. To receive cover under Pool Re, an official confirmation that an act of terrorism has taken place must be agreed by the U.K. Government, which issues a certificate under an agreed procedure, as established in [EU1].

Rather than establishing a private company, the U.S. chose to pass the Terrorism Risk Insurance Act (TRIA) of 2002 in response to the 9/11 terrorist acts. Kunreuther and Michel-Kerjan (2004) outline how TRIA obligated insurers to offer terrorism coverage with identical limits and deductibles to non-terrorism coverage. If the U.S. Treasury Secretary certifies the event as an 'act of terrorism', then the losses will be shared by the Federal Government and insurers according to a pre-agreed format up to U.S.$100 billion; beyond that, the Treasury determines how losses are to be divided. The U.S. Treasury does not charge a premium for coverage; rather, it recoups funds via mandatory surcharges on specific insurance policies.

We now outline the options within such a scheme, by contrasting the U.S. and the U.K. approaches. Such a scheme can *collect funds ex-ante (Pool Re) or ex-post (TRIA)* (4.6.2); Pool Re collects the premiums into a central fund used in the event of a catastrophic loss, while TRIA recovers funds ex-post. Second, *membership can be optional (Pool Re) or mandatory (TRIA)* (4.6.3).

Another consideration is whether the *premium is priced according to underlying risk (Pool Re) or according to the amount of insurance sold (TRIA)* (4.6.4). In the DHS working group, it was suggested that intelligence information collected by government agencies cannot be released for national security reasons. A government playing the role of re-insurer of last resorts allows this information to be priced into the market. Doing so is particularly effective in the Pool Re model where the U.K. Government is involved in negotiating the price of premiums to join the scheme.

Brice (1994) suggests that the risk is not adequately spread through the economy in these schemes. This problem is compounded by the nature of cyber risks. Under Pool Re, the U.K. Government is only liable for property in the U.K. However, [LL2] showed that 94% of the cyber premiums received by the Lloyd's market comes from organisations based outside the U.K. This problem underlies the majority of schemes; in effect one government holds liability for global cyber risks.

A number of alternative systems to Pool Re that provide limits to the amount of risk a government holds are outlined by Brice (1994). A government can place an *upper limit on the amount the scheme will cover* (4.6.5). This approach is used in Sri Lanka where the Strike,

Riot, Civil Commotion and Terrorist model caps the amount it will cover relating to a terrorist act. It is suggested that re-insurance firms may feel comfortable insuring losses beyond the cap.

Alternatively, a government can place an *upper limit on the amount one insured can claim* (4.6.6). The Overseas Private Investment Corporation (OPIC), which was set up by the U.S. to underwrite political risk in developing countries, places a cap on the amount of cover an individual insured can purchase at 10% of OPIC's total liability. Such a cap could mitigate governments holding liability for risk associated with major service providers, which was repeatedly raised as a major point of risk aggregation in the interviews.

4.7. Summary

Our results suggest a number of policy measures that address the challenges related to each theme. Responses to promote wide adoption (Section 4.1) can only be enacted by governments as they involve legislation or the processes of government agencies. Meanwhile, efforts to encourage exclusions or standardise coverage (Section 4.2) are reliant on the cooperation of individual insurers. Such interventions are dependent on stakeholders' interests being aligned and this motivates our stakeholder analysis. For example, we identified that governments desire standardised coverage as it produces consistent data for analytical purposes, but insurers see tailoring coverage as part of the service they offer.

Collective action problems, such as the race-to-the-bottom in assessment standards identified in Section 4.3, should be priority areas for intervention whether that is led by government or by a coalition of insurers. Other interventions require leadership on the part of governments, such as defining best practice (Section 4.5) or mandating other industries to make data available (Section 4.4). Finally, the role of government as insurer of last resorts outlined in Section 4.6 is the weightiest intervention and, as such, necessitates the deepest consideration. The next section draws together the stakeholder analysis and discusses the viability of each policy measure.

5. The framework

In Section 5.1, the results of the stakeholder analysis are presented for each intervention option, providing an idea of how viable that intervention is. A recently published report is used to validate the framework in Section 5.2. In Section 5.3, we outline a research roadmap linking this framework to future work that could support a public–private partnership for cyber insurance.

5.1. Presentation of framework

Our findings inform the framework presented in Table 2. We will give a brief overview of each policy item in turn.

For wider adoption (*Theme* 1), no stakeholder suggested that legislation assigning a financial cost (1.1) should be created to increase demand for cyber insurance. Raising awareness about gaps in traditional policies (1.2) is the role of brokers, who should need no incentive to sell more insurance; as such, it would not be appropriate for a government to intervene. The only consideration was whether the forthcoming GDPR fines

Table 2. A framework to describe possible policy measures affecting the cyber insurance market.

Theme	Policy measures
1. Wider adoption	1.1 Legislation creating a financial cost to cyber events [EU1, EU2, UK1, US1, US4]
	1.2 Raise awareness about gaps in traditional insurance products [EU1, EU2, US1, UK1]
	1.3 Governments to exercise their procurement power to support market development [EU1, UK1, US1]
	1.4 Mandate insurance for organisations in certain industries [US4]
2. Defining coverage	2.1 Encourage the use of cyber exclusions in non-cyber policies [UK1, US1, US4]
	2.2 Standardise wording of cyber insurance policies [EU2, US1]
	2.3 Provide certification for acts of cyber war or terrorism [EU1]
3. Data collection	3.1 Standard data formats for assessment or claims process [UK1, US1, US4]
	3.2 Minimum standards for data collection in assessment process [US2]
	3.3 Government collects high-level data on the insurance market [EU1, US1]
4. Information sharing	4.1 Make data held by government agencies available [US1, US2, US4]
	4.2 Open up access to existing information-sharing initiatives [UK1]
	4.3 Mandate other organisations to make data available [US1]
	4.4 Government to create a cyber incident data repository [US1, US4]
5. Best practice	5.1 Government can define information security best practice [UK1, US1, US4]
	5.2 Lead organisations to best practice through regulation [EU2, US4]
	5.3 Clarify liability related to insurers giving security advice [EU1, US4]
6. Catastrophic loss	6.1 Government to act as insurer of last resorts [EU1, UK1, US1]
	6.1.1 Collect funds ex-ante [Pool Re] or ex-post [TRIA]
	6.1.2 Joining scheme is optional [Pool Re] or mandatory [TRIA]
	6.1.3 Premium priced according to underlying risk [Pool Re] or priced according to amount of insurance sold [TRIA]
	6.1.4 Upper limit on the amount the government will cover [Sri Lanka]
	6.1.5 Upper limit on the amount one insured can claim [OPIC model]

should be insurable or not. Using the procurement process to influence cyber insurance take-up (1.3) is not well supported. Meanwhile, ENISA actively recommend against mandatory cyber insurance (1.4). Measures to increase the size of the market are not as urgent given that some estimates[12] predict annual premium sales will reach U.S.$5 billion by 2018 and at least U.S.$7.5 billion by 2020.

Defining coverage (Theme 2) is an area with little divergence in interests. All stakeholders believe exclusions (2.1) provide clarity and should be encouraged. The Lloyd's market has pre-existing efforts to spread their usage. The case is less clear with producing standard definitions for coverage wordings (2.2); while more standardisation would improve data for analytical purposes, insurers feel tailoring coverage to the applicant is part of their service offering. There is cross-stakeholder support for clarification on what constitutes cyber war or terrorism (2.3), which could be provided by a government.

Data collection (Theme 3) tends to be supported by all stakeholders. Governments should work with insurers to define standard data formats (3.1) and establish a minimum standard of assessment and data collection (3.2); this will produce better actuarial data and also avoid the race-to-the-bottom on depth of assessment. If the consultation is sufficient, there should be little industry resistance. Though the ENISA report identified governments as being best placed to collect high-level market data, we suggest that work should be done in consultation with organisations such as Lloyd's or regulators, as they already collect data on the size of insurance markets (3.3). Finally, any of the measures to widen coverage would increase the volume of data, which includes mandatory coverage (3.4).

Information sharing (Theme 4), though supported in principle, tends to be opposed by those stakeholders who are expected to share information: governments resist

making data available (4.1) on national security grounds; large insurers oppose making their data available (4.3) as they see their claims data as a competitive advantage. One achievable option is for governments to ensure that insurers have access to existing information-sharing institutions (4.2). Efforts to construct a cyber data repository (4.4) are ongoing in the U.S.,[13] with a recent update suggesting a proof of concept is being built.

Interventions to help the insurer propagate best practice (Theme 5) have two components. The first component (5.1) concerns what defines best practice, with a candidate being the NIST standard;[14] whether there needs to be consensus on this is not clear. However, interviewees revealed that the controls they are concerned about are driven by the claims they see, rather than by existing standards. To incorporate both stakeholders' contributions, policy-makers can define a minimum standard through existing legislation (5.2), while insurers provide additional guidance based on the dynamic threat landscape. The second component is the ability of the insurer to spread best practice. The liability an insurer faces for recommending certain risk controls should be clarified (5.3).

Finally, the challenge of catastrophic loss (Theme 6) motivates a consideration of governments playing the role of insurer of last resort. We suggest that pricing premium contributions according to underlying risks (6.1.3) allows governments to price their threat intelligence into the market, without compromising national security. Further, an upper limit on the amount an individual policy can claim (6.1.5) could be advisable given the monopoly of certain service providers; governments holding liability for this risk supports that monopoly. However, there does not seem to be much will among the policy-making community to make such a scheme happen. Previous schemes were only implemented after catastrophic events and it is likely that it would take a cyber equivalent to force the governments' respective hands.

5.2. Validation

In 2017, a report entitled *Supporting an effective cyber insurance market* by the OECD (2017) was presented to the G7. As the motivation for that report is similar to ours, we use its content as a means of validating our findings.

Four challenges are identified in the report: limited exposure; misunderstanding in coverage available; uncertainty about exposure; and risk of correlated exposure. Figure 1 demonstrates how our themes map to those challenges.

The report also suggests three policy priorities. The first is to understand impediments and gaps in the market; this relates to our theme of defining coverage (Theme 2) and the policy measure collecting high-level data on the insurance market (3.3). The second is to improve public policies to manage cyber risk, which corresponds to leading organisations to best practice through legislation (5.2).

The third policy priority relates to developing a comprehensive data set on cyber incidents. It identifies the following policy measures: creating common classification of cyber incidents, which relates to (3.1); creating incentives or requirements for information-sharing, which relates to (4.3); and establishing a trusted party (e.g. a government agency) to collect and report the data. The final recommendation is one of the three objectives of the DHS working group and is extensively discussed in [US4].

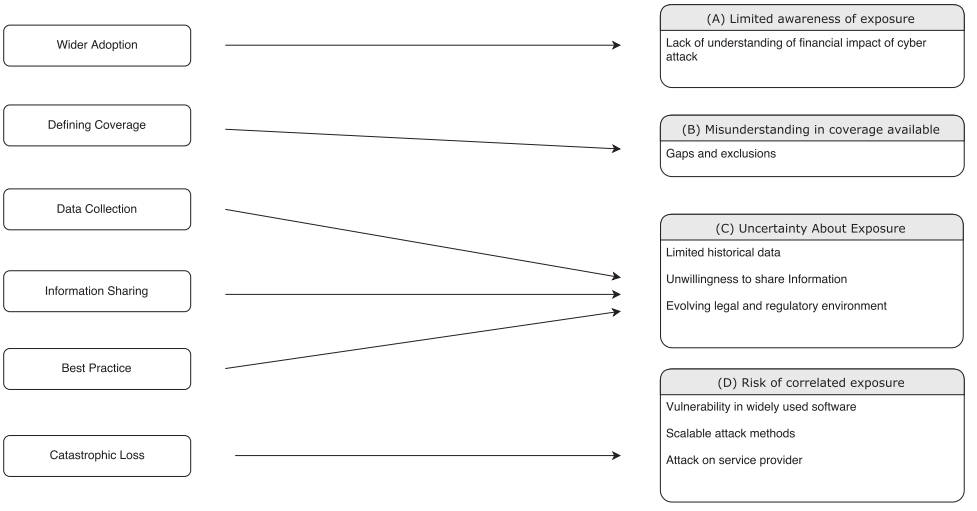

Figure 1. Mapping the themes constituting the framework to the challenges identified in the OECD report.

The report and our study identify similar challenges to the market. However, the OECD report emphasises challenges typically associated with an immature market and the corresponding responses. The framework does not overlook these challenges: the policy measures related to Themes 1 and 2 are focused on wider adoption and clarifying coverage, respectively, both concerns of an immature market.

The influence from the U.S. and the U.K., both of whose markets display higher maturity, led us to consider the processes of a functioning insurance industry, such as how insurers collect and share data or the security recommendations they provide. Consequently, our framework provides a number of policy measures relevant to a mature market. While these are not presently relevant for markets with limited cyber insurance adoption, the later themes in the framework will have increasing relevance as the global market matures.

5.3. Research roadmap

The presented framework can inform research directions into the policy measures that might constitute a cyber insurance public–private partnership. Future work could expand our stakeholder analysis to include cyber insurance customers. Ultimately, policyholders will be the actors who implement cyber security measures. Further, they play an important role in determining the scope of the insurance offered, which could include reputational harm or class-action law suits. These differences in coverage motivate an investigation into how each product affects the management of cyber security.

The legal scholarship can continue to inform the wording of coverage (Theme 2), as seen in the work of Beh (2001) and Crane (2001). This work will be important as, for example, the so-called Iinternet of Things sees cyber risks impact tangible property. The questions of what constitutes information security best practice (Theme 5) remain unsolved despite the continued efforts of the research community; the insurance industry should attempt to apply advances where possible. In addition, the insurance industry can

provide researchers with another source of data to support this research. Researchers could define how to collect assessment and claims data (Theme 3) in order to move towards a more empirical underpinning of security research, which Verendel (2009) has suggested is lacking.

Both Brice (1994) and Kunreuther and Michel-Kerjan (2004) have explored the role of government as insurer of last resort in relation to risks arising from terrorism; we suggest that future work is needed to understand how such schemes can cover cyber risks. Böhme and Schwartz (2010) provide an overview of models for aggregated cyber risk; advances in this area would support the understanding of catastrophic loss (Theme 6). Kunreuther and Michel-Kerjan (2004) showed that the time between the catastrophic incident (9/11) and the policy response (passing TRIA) was minimal. Consequently, research should be conducted, even if at present it is not an area of concern.

We anticipate further developments within academia and the policy-making community that will extend the range of policy measures under consideration. We hope that this framework can serve as a first step towards a holistic consideration of a public–private partnership for cyber insurance.

6. Conclusion

Non-tangible digital assets and the dynamic nature of cyber attacks present novel challenges to the insurance industry and governments alike. There are a number of policy measures that can address these challenges and support an effective cyber insurance market. Together such measures can underpin a public–private partnership for cyber insurance. This paper presents a framework to identify the constituent parts of such a partnership, together with a research roadmap to help develop deeper understanding of these issues.

Our analysis reveals that wider adoption and defining coverage should not be priorities as the market is expanding and the wording of coverage is already being addressed by the insurance industry. Data collection efforts provide an opportunity for a welcome intervention by government: they can work with the industry to define standard data formats, establish minimum assessment standards and collect high-level data. Conversely, information-sharing initiatives are likely to be resisted by certain stakeholders.

Propagating best practice will again require coordination, and we suggest that regulation can establish minimum standards and that insurers request additional controls in response to the claims they see. Finally, while we would argue that governments should not yet accept the role of insurer of last resort, we suggest that investigating the feasibility of this should be a priority area for the research community.

Notes

1. Cyber-Insurance Metrics and Impact on Cyber-Security, Internet Society Alliance: http://bit.ly/2oFIQli
2. PWC, Insurance 2020 and beyond: Reaping the dividends of cyber resilience: http://pwc.to/2ppT17P
3. Hiscox: http://bit.ly/2pvSUbK
4. See https://www.lloyds.com/lloyds/offices/americas/us-homepage/about-us
5. http://bit.ly/2pBaiY8

6. http://bit.ly/2plBNJD
7. http://www.eugdpr.org/
8. See https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017
9. https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/
10. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
11. https://www.poolre.co.uk/what-we-do/
12. PWC, Insurance 2020 and beyond: Reaping the dividends of cyber resilience: http://pwc.to/2ppT17P
13. NextGov, http://bit.ly/2plkYrQ
14. See http://bit.ly/2ePWDZM

Acknowledgements

The authors are grateful to the anonymous reviewers and the editor for their helpful and constructive comments. In addition, the authors would like to thank Willis Towers Watson for facilitating the interviews and the participants for volunteering their time.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

The first author would like to acknowledge the support of the EPRSC in funding (EP/P00881X/1) his place at the Cyber Security Centre for Doctoral Training (CDT).

Notes on contributors

Daniel Woods gained an M.Sc. in Mathematics from the University of Bristol, United Kingdom. Following that he joined the Cyber Security Centre for Doctoral Training at Oxford University. The CDT programme consists of one year of intensive education in cyber security, followed by three years of research. The centre takes a multidisciplinary approach and introduces the challenge of Cyber Security from a range of academic perspectives.

Andrew Simpson gained a first-class honours degree in Computer Science from the University of Wales, Swansea. Later, he received an M.Sc. and a D.Phil. from the University of Oxford. He is currently a University Lecturer in Software Engineering at the University of Oxford, teaching on the Software Engineering Programme. Previously, he was a Principal Lecturer in Computing at Oxford Brookes University; prior to that he was a research officer in the Computing Laboratory (now Department of Computer Science).

ORCID

Daniel Woods http://orcid.org/0000-0002-8569-1917

References

Beh, H. G. 2001. "Physical Losses in Cyberspace." *Connecticut Insurance Law Journal* 8: 55.
Böhme, R., and G. Schwartz. 2010. "Modeling Cyber-insurance: Towards a Unifying Framework." Proceedings of the Workshop of Economic Information Security (WEIS) 2010.

Brice, W. B. 1994. "British Government Reinsurance and Acts of Terrorism: The Problems of Pool Re." *Pennsylvania Journal of International Business Law* 15: 441–468.
Camillo, M. 2017. "Cyber Risk and the Changing Role of Insurance." *Journal of Cyber Policy* 2 (1): 53–63.
Crane, M. 2001. "International Liability in Cyberspace." *Duke Law & Technology Review* 1 (1): 23–29.
ENISA (The European Union Agency for Network and Information Security). 2012. "Incentives and Barriers of the Cyber Insurance Market in Europe." http://bit.ly/2qXUUd7.
ENISA (The European Union Agency for Network and Information Security). 2016. "Cyber Insurance: Recent Advances, Good Practices and Challenges." http://bit.ly/2fNiQIC.
Kesan, J., R. Majuca, and W. Yurcik. 2005. "Cyberinsurance as a Market-based Solution to the Problem of Cybersecurity: A Case Study." Proceedings of the Workshop of Economic Information Security (WEIS) 2005.
Kunreuther, H., and E. Michel-Kerjan. 2004. "Policy: Watch Challenges for Terrorism Risk Insurance in the United States." *Journal of Economic Perspectives* 18 (4): 201–214.
Majuca, R. P., W. Yurcik, and J. P. Kesan. 2006. "The Evolution of Cyberinsurance." *arXiv preprint:cs/0601020*.
OECD (Organisation for Economic Co-operation and Development). 2017. "Supporting an Effective Cyber Insurance Market." http://bit.ly/2qobHF9.
Schneier, B. 2001. "Insurance and the Computer Industry." *Communications of the ACM* 44 (3): 114–115.
UK Cabinet Office. 2015. "UK Cyber Security: The Role of Insurance".
US Department of Homeland Security. 2012. "Cybersecurity Insurance Workshop Readout Report." Accessed February 27, 2017. http://bit.ly/2qY8MUW.
US Department of Homeland Security. 2013. "Cyber Risk Culture Roundtable Readout Report." http://bit.ly/2qdfraY.
US Department of Homeland Security. 2014a. "Healthcare and Cyber Risk Management: Cost/Benefit Approaches." http://bit.ly/2pFjhl0.
US Department of Homeland Security. 2014b. "Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues." http://bit.ly/1nZC0wM.
Verendel, V. 2009. "Quantified Security is a Weak Hypothesis: A Critical Survey of Results and Assumptions." Proceedings of the New Security Paradigms Workshop (NSPW) 2009: 37–50. ACM.
Von Solms, B., and R. Von Solms. 2004. "The 10 Deadly Sins of Information Security Management." *Computers & Security* 23 (5): 371–376.