ASSESSMENT OF THE CYBER INSURANCE MARKET

DECEMBER 21, 2018

CISA
CYBER+INFRASTRUCTURE

Table of Contents

List of Acronyms

AI	Artificial Intelligence
AIR	AIR Worldwide
CIAB	The Council of Insurance Agents & Brokers
CIRI	Critical Infrastructure Resilience Institute
CISA	Cybersecurity and Infrastructure Security Agency
CyRiE	Cyber Risk Economics
DHS	U.S. Department of Homeland Security
NIST	National Institute of Standards and Technology
NRMC	National Risk Management Center
NSTAC	National Security Telecommunications Advisory Committee
OCE	Office of the Chief Economist
OECD	Organisation for Economic Co-operation and Development
RMS	Risk Management Solutions
S&T	Science and Technology Directorate
SEC	U.S. Securities and Exchange Commission
SEM	Stakeholder Exchange Meeting

1. Objectives and Outline

1.1. Objective

The U.S. Department of Homeland Security's (DHS) National Risk Management Center (NRMC) within the Cybersecurity and Infrastructure Security Agency (CISA) requested that CISA's Office of the Chief Economist (OCE) assess the current state of the cyber insurance market. The aim of the assessment is to (1) analyze the cyber insurance market to understand the most current trends and challenges and (2) identify relevant efforts related to cyber insurance that could inform NRMC research and collaboration agenda and aid prioritization of requirements.

1.2. Report Outline

The remainder of this paper is organized as follows. Section 2 provides a summary of the results. Section 3 describes the sources and methods used by OCE for this analysis. Section 4 includes the analysis and a summary of the findings. Section 5 analyzes which potential efforts could be considered as part of NRMC long-term collaboration priorities. Section 6 contains the conclusions. A list of suggestions for further research and follow-up activities is included in Appendix A. Appendix B describes programmatic efforts DHS has already undertaken related to cyber insurance.

2. Results in Brief

Based on the academic literature and information from DHS partner programs in CISA and the Science and Technology Directorate (S&T), OCE found that the cyber insurance market remains underdeveloped despite significant growth over the last 2 years. OCE found that there are three core challenges that constrain the cyber insurance market: a lack of data, methodological limitations, and a lack of information sharing. These core challenges limit the market's development and any actions the federal government can take to effectively advance solutions.

3. Sources and Methods

OCE conducted a literature review to characterize the current state of the cyber insurance market. In doing so, OCE sought to balance the perspective of the research community with observations offered by private-sector practitioners and industry publications, and to identify the extent to which progress has been made in resolving challenges identified in the literature or proposing innovative solutions in the period from 2016 to 2018.

In addition to conducting a literature review based on publicly available sources, OCE gathered information from DHS programs that address the cyber insurance market. The information from the DHS programmatic activities helped OCE to validate the issues identified in the literature review. For a brief description of these DHS programs, please refer to Appendix B.

4. Analysis

An assessment of the challenges faced by the cyber insurance market is necessary to understand both its current state and the potential role it can play in improving cybersecurity. The following subsections address these two issues. Section 4.1 provides a purely descriptive characterization of the current state of the market by listing the core challenges in the market (i.e., a lack of data, methodological limitations, and a lack of information sharing) and describing the implications of

those challenges. In Section 4.2, OCE explores the role the cyber insurance market could have in improving cybersecurity if it were more fully developed.

4.1. Current State of the Cyber Insurance Market

Although cyber insurance products have been on the market since the late 1990s, the market is still in its infancy (Aon Inpoint, 2017). Aon Inpoint estimates that while 75 percent of financial institutions, retail, health care, and hospitality companies with revenue over $1 billion purchase some cyber insurance, fewer than 5 percent of small and medium businesses are consumers in the market. According to the Council of Insurance Agents & Brokers (CIAB, 2018), the overall cyber insurance take-up rate was approximately 32 percent over the first half of 2018.

CIAB (2018) and PwC (2018a) characterize the current state of cyber insurance as a soft market with excess capacity due to an influx of new insurers entering the market. Nearly 89 percent of respondents to the CIAB (2018) survey indicated that their premiums remained either flat or decreased over the first half of 2018. The Marsh (2018) third-quarter U.S. Cyber Insurance Market Index shows similar statistics over the previous 5 quarters.

A.M. Best (2018a) states that the number of direct premiums written increased to $1.8 billion in 2017 (i.e., a 32 percent increase from 2016). The number of policies in force increased by 24 percent to 2.6 million. However, the growth is attributed to companies reclassifying policies for reporting purposes or adding cyber coverage or exclusions to existing policies. As far as standalone cyber policies, there was a 32 percent decline attributed primarily to firms choosing cheaper packaged policies.

According to A.M. Best (2018b), the top four leaders in underwriting were Chubb INA Group, the American International Group, the XL Catlin America Group, and the Travelers Group. The Hartford Insurance Group held the most cyber policies in force by the year's end, with more than half a million policies (Business Wire, 2018). However, the Hartford Insurance Group is 13th in underwriting according to A.M. Best (2018b), with about $25 million in direct premiums written in 2016 and approximately $35 million in 2017. This implies that relatively cheaper premiums and lower coverage policies dominate the market, as indicated by the cyber policies in force metric. The dominance of cheaper policies in the market is also reflected by the comparative statistics on purchasing from the Marsh Global Analytics Group (personal communication, 2018). However, a recent study found that although

> "the demand for cyber insurance is growing, [...] insurers are wary of expanding coverage due to lack of credible data, interdependent security, asymmetric information issues such as adverse selection and moral hazard, and the potential for catastrophic aggregate losses in the face of correlated exposures among policyholders. The result is cyber insurance policies with gaps in coverage and lower limits that do not indemnify insureds for many cyber losses" (Shetty et al., 2018, p. 235).

This is also consistent with the J.D Power (2017) 2017 Large Commercial Insurance Study Rankings, which show that of all the available insurance programs, the cyber insurance line is consistently rated lowest.

The number of cyber claims grew by 51 percent from 5,955 in 2016 to 9,017 in 2017 (Business Wire, 2018). Only 28.4 percent of closed claims resulted in payments, and the average closed claim

with payment was approximately $188,525 for standalone policies (Bermuda:Re+ILS, 2018). Although data on the full range of payment magnitudes are not available, OCE estimates there was an overall payout of approximately $483 million in 2017.[1] This constitutes only about 27 percent of the 2018 underwriting volume.

Low limits and payouts, along with the 2018 underwriting trends, indicate that while cyber insurance customers are buying more cyber insurance with higher limits than in the previous 2 years, they are not getting what they want.

In Section 4.1.1, OCE describes the core challenges with the current state of the cyber insurance market that were outlined in the most recent literature as well as lessons learned drawn from DHS cyber insurance efforts.[2]

4.1.1. Core Challenges

In general, both the literature and related DHS efforts identify the following three overarching challenges associated with the cyber insurance market: a lack of data, methodological limitations, and a lack of information sharing. These core challenges create significant difficulties for decision makers in understanding, assessing, and managing cyber exposure.

The theoretical academic literature prioritizes information asymmetry, interdependent security, and correlated losses as the three main challenges.[3] Meanwhile, applied research and industry publications emphasize the lack of quality data and tested cyber exposure models as the key obstacles, which in turn make it difficult to properly assess risks, structure coverage, and price premiums.[4]

The challenges identified in the academic literature and industry publications are closely related. Interdependent security and correlated losses complicate the development of theoretical models that would accurately capture the relationship between various characteristics of the entity, its security posture, current cyber threats, and potential losses. In turn, the lack of data prevents insurers from meaningfully quantifying the limited models available and deriving correlations between multiple factors to inform further model development. OCE provides a more detailed overview of the three core challenges below.

Lack of Data

The most commonly cited challenge with the cyber insurance industry is the lack of historical loss data, which limits the development of cyber loss modeling to quantify the risk and affects the

---

[1] $483 million in payouts = 9,017 claims × 28.4% of claims resulted in payouts × $188,525 per payout.

[2] For more details on the challenges faced by the cyber insurance industry, refer to the following articles. Marotta, Martinelli, Nanni, Orlando, and Yautsiukhin (2017) provide a plain language overview of the cyber insurance market including explanations of basic terms, descriptions of current issues in the cyber insurance industry, and a host of citations to articles providing more details on each of the issues. Risk Management Solutions, Inc. (RMS, 2016) developed a more technical overview of current underwriting and risk selection practices in cyber insurance.

[3] For more details, see Khalili, Liu, and Romanosky (2018) and Pal (2012).

[4] For more details, see A.M. Best (2018b), Bermuda:Re+ILS (2018), PwC (2018a), and Romanosky et al. (2017).

perception of decision makers with respect to the anticipated likelihood and magnitude of cyber losses.

A PwC (2018a) survey indicates that insurance companies have an average of 7 years of cyber insurance claims data available to support underwriting and modeling. Claims data are typically available for only limited types of cyber incidents, such as breaches, ransomware, malware, and phishing. In addition to the data that insurance companies have from their own customer claims, there are four main commercially available sources of the incident and loss data: Advisen, RBS, NetDiligence, and SASOpRisk. Advisen and NetDiligence have the greatest number of observations on costs and losses, with the majority of their data being related to data breaches.[5] In comparison to the more than one hundred years' worth of data on events and losses that risk modelers rely on for assessing potential losses from other perils (e.g., floods and other natural hazards), the amount of data on cyber-related incidents is extremely limited.

The Organisation for Economic Co-operation and Development (OECD, 2018) states that a cause of the lack of data may be that relatively few cyber incidents have been discovered. The detection and discovery rate is a recognized limitation in cybersecurity as the body of knowledge on cyber losses would be limited to only what is observed. It is unclear what portion of the total adversarial activity (i.e., all observed and unobserved events) is represented by the observed adversarial activity. Clearly, events that are not discovered would not result in attributable realized losses; hence, no claims would be filed. However, the issue emphasized here is a lack of specific data on observed events that go unreported, or for which losses are undisclosed. The lack of data on observable events is also due to the general and non-binding disclosure and reporting guidance for private sector entities with respect to discovered cyber incidents.[6]

Statistics from the most recent Data Breach Investigation Reports (Verizon, 2018, 2019) show that there is a significant difference in incident reporting between the public sector, where the incident reporting requirements are clearly defined, and the private sector, where the reporting guidance is more ambiguous. Verizon (2018) shows that 22,429 large incidents were reported for the public sector, while the private sector in its entirety reported only 1,033 large incidents.

While the public sector seems to have better incident reporting requirements and reporting mechanisms, the losses attributed to reported incidents are not easily tracked or estimated. In the private sector, tangible realized losses are accounted for, and the damage totals that pass the U.S. Securities and Exchange Commission (SEC) materiality threshold are disclosed in SEC filings. Damage totals are also submitted to insurers as part of the claims process, but only rarely are they communicated publicly in a sufficient level of detail to itemize costs and losses.

The limitations of data availability discussed above do not take into account the ever-changing threat environment that makes underwriting cyber risk different from traditional property and casualty underwriting. Eling and Schnell (2016) argue that the usefulness of historical data is limited by how quickly the environment for cyber risk changes. Marotta et al. (2017) state that attackers are highly adaptable in terms of their attacks; thereby making it very difficult to predict

---

[5] NetDiligence (2018a) had data on approximately 1,200 claims from 2013 to 2017, while Advisen had data on approximately 1,500 claims from 2005 to 2017 (S. Romanosky, personal communication, 2018).

[6] For more details on the U.S. Securities and Exchange Commission (SEC) disclosure and reporting guidance, see SEC (2011).

changes. Therefore, the duration that historical data remains relevant for quantifying cyber risk and determining premiums is short (Shetty et al., 2018; PwC, 2018a).

In addition, a lack of data has an impact on risk perception, which significantly influences the decision to pursue cyber insurance coverage. De Smidt and Botzen (2018) surveyed corporate professionals engaged in risk and insurance decision making at mainly large companies and found that these professionals tend to overestimate the probability of a successful cyber attack, while underestimating the financial impact. This may explain the reluctance to seek cyber insurance.[7] Businesses have difficulty appreciating what insurance can and should do given that cyber incidents do not happen frequently enough (Cyber Risk Economics [CyRiE], personal communication, 2017). There are multiple reasons for this, but availability and the quality of the data on both cyber incidents and resulting losses are some of the limiting factors heavily influencing perceptions of cyber risk by the decision makers (A.M. Best, 2018b).

Finally, even if cyber risk quantification were sufficiently mature to align policy pricing and underwriting with the commensurate amount of risk, and the legal environment had a sufficient number of precedents to more clearly guide compensation practices, policyholders might still be reluctant to file claims. Businesses may be hesitant to file claims because an investigation is often required following an incident (Marotta et al., 2017). A public investigation puts a burden on the business and it can hurt its reputation, thereby exposing it to additional, uncovered losses. Damage to reputation is one of the recognized obstacles with filing claims and disclosing cyber incidents or breaches.

Methodological Limitations

The second core challenge hindering the maturation of the cyber insurance market is methodological. This challenge is related to the limitations of the existing models for assessing cyber risk, namely a lack of robust and reliable cyber loss quantification models that can be calibrated to historical data and validated on an ongoing basis. There are four major reasons why cyber risks are exceptionally difficult to model, and hence, to underwrite: (1) intangible costs, (2) the ever-changing threats from intelligent adversaries, (3) correlated risks, and (4) interdependent security.

First, Marotta et al. (2017) state that it is difficult for insurers to estimate the potential damage from cyber events because many of the costs are intangible (e.g., loss of reputation), and the nature of the assets at risk include things such as intellectual property and private identifiable and heath information. The costs, losses, and consequences can vary significantly based on the type of event that occurs and the impacted asset.

Second, modeling is further complicated by the need to account for an intelligent adversary, where behavior, methods, and targets constantly evolve. The adversary-driven dynamic nature of cyber risk differentiates it from all other events typically covered by insurance policies.

Third, according to Marotta et al. (2017), insurers are particularly at risk in the cyber space, because several policyholders can be impacted at the same time (e.g., due to worms, bugs, and

[7] Refer to the de Smidt and Botzen (2018) article for more details on the behavioral factors (e.g., the availability heuristic, threshold level of concern, degree of worry, and trust in organizational capabilities) that they found to have a significant influence on the perceived probability and impact of cyber attacks.

botnets). Correlated risks are particularly likely in the cyber environment, because of the similarity of computer systems across the globe. Attacks can be easily and cheaply performed on several systems at the same time. Therefore, insurance companies need to have a good understanding of the magnitude of losses and damages from a single event not just for individual policyholders, but how these losses and damages are correlated and can propagate through a group of policies within a portfolio. The depth, breadth, and rate of WannaCry and NotPetya's propagation are the most recent examples of how the scale of damages from a single campaign can quickly change and accumulate (Hern, 2017). This is known as accumulation risk.[8] It significantly complicates loss modeling, which in turn, influences the ability of insurers to structure coverage, adjust limits, and determine price premiums. Risk accumulation is hard to diversify, because reinsurers suffer from the same challenges as primary insurance companies in assessing risks and solvency, and are hesitant to expand cyber risk reinsurance product lines (OECD, 2018). PwC (2018a) and RMS (2016) indicate that setting parameters for probable maximum loss is a key challenge in managing cyber accumulation.

Fourth, interdependent security is a feature of the cyber network system because an individual's level of security also depends on actions of others, over which it has no control (Kunreuther & Heal, 2003). Because systems are connected to other systems, individual decisions of each participant in the network impact the collective level of security. An individual entity's may suffer consequences due to the actions of others (i.e., a negative externality). Because interdependent security creates negative externalities and has a potential to introduce, scale up, and proliferate losses throughout entire portfolios, it amplifies accumulation risk. Interdependent security is also related to systemic risk. It provides pathways for severe shocks and damages to propagate through an interconnected and interdependent system to the point that it can threaten to collapse the entire system.

Lack of Information Sharing

The third core challenge is a lack of information sharing. Policyholders are hesitant to disclose information about their incidents, costs, and losses, while insurance carriers are reluctant to share among themselves the damage and claims data from their customers. Furthermore, there are also barriers to information sharing within organizations.

Factors hindering data sharing can be broadly categorized into trust, privacy, legal, and financial issues (Day, 2018). This is not a phenomenon unique to the cyber insurance market. It is also present in other sectors, where the benefit of voluntarily sharing data is collective; however, the costs and risks (actual or perceived) of meaningfully contributing data are disproportionately borne by the few individual contributing entities. For example, a major reason organizations are hesitant to share information is that they do not want to reveal their vulnerabilities, for fear that it could negatively affect their business or their reputation. Marotta et al. (2017) and Romanosky, Ablon, Kuehn, and Jones (2017) state that this secondary impact, damage to reputation, is often not covered by cyber insurance policies.

The lack of information sharing results in information asymmetry, where the risks are better known to the policyholder than the insurer (Ligon & Thistle, 1996). In addition, insurers face a moral hazard problem as is difficult for insurers to monitor if policyholders are protecting themselves from cyber risks (Marotta et al., 2017). Once insurance is in place, policy holders may

[8] For more details on accumulation risk, see RMS (2016).

not make updates to their controls or use their controls effectively. Some may reduce their investment in cybersecurity as they expect the insurance to cover any losses. This is not an unlikely scenario, because other moral hazard symptoms have already surfaced as part of CIAB (2018) survey. Namely, some of the suggested incentives for accelerating cyber insurance market in the survey had to do with reducing or eliminating fines and penalties for failing to protect client data, if the company has cyber or privacy coverage in place.

Information asymmetry makes it difficult for insurers to determine a risk-based premium (Shetty et al., 2018). The lack of information sharing also exacerbates the issue of data availability: not only is there a lack of a historical data, there is not an effective data collection or data sharing mechanism in place that could alleviate the sparsity of data over time.

Information asymmetry not only occurs between policyholders and insurers. De Smidt and Botzen (2018) also found that there is internal information asymmetry within organizations as senior management largely rely on the opinion of information communication technology staff when it comes to the technical aspects of cybersecurity. As information about vulnerabilities, security posture, and potential cyber risks floats upward—from the tactical level to the operational level and then to the strategic level—to support the risk assessment and risk management decisions by senior management, it becomes increasingly aggregated and opaque.

Even technical cybersecurity staff, in providing this information to senior management, grapple with an incomplete understanding of potential cybersecurity issues, because the software market is characterized by a degree of uncertainty about the quality of the products. In economics this is known as the market for lemons (Akerlof, 1970), where the buyers of the software or cybersecurity products do not have full information about the value and security state of the product.

Further, often even the vendors themselves do not have full knowledge of how secure the software is (Pal, 2012; Anderson & Moore, 2009). The product development cycle emphasizes the release schedule, with the subsequent discovery of vulnerabilities and the resulting issuance of patches, bug fixes, and updates being the norm in such a fast-paced industry. Therefore, cyber risk management at the operational level becomes a random walk from one set of newly discovered vulnerabilities to the next across a myriad of products.

4.1.2. Implications of the Core Challenges

The problems listed above are caused by a lack of relevant historical data, methodological limitations, and issues with data sharing. These challenges impede the evolution of cyber policy product lines because cyber risk cannot be quantified in a reliable and robust manner. Therefore, insurers have difficulties pricing policy premiums, which makes cyber risk exceptionally difficult to underwrite in a way that is commensurate with potential losses.

This issue manifests itself in other aspects of the cyber insurance market, specifically in establishing types of coverage, defining limits, and pricing premiums. Thus, it leads to overlapping coverage between cyber insurance and other insurance policies, limited cyber insurance coverage, a wide variability in coverage specification, low indemnity limits, and a number of legal questions surrounding liability and compensation practices. All of these factors lead to a low overall cyber insurance holding rate (CIAB, 2016a, 2016b, 2017, 2018; PwC, 2018a), although the uptake has increased significantly in 2018 (A.M. Best, 2018a; Marsh, 2018).

Policy Premium Pricing

By examining insurance policies, Romanosky et al. (2017) attempted to understand the underlying approach to risk assessment and how it relates to premium calculations. Their assessment shows that there is wide variation in the methods used for pricing premiums, with significant differences in the sophistication of the equations and the metrics used for quantification. The pricing methods ranged from basic, flat-rate pricing, to methods that attempted to account for the policyholder's level of cybersecurity by incorporating information on their controls and practices.

Even the most sophisticated policies relied only on the self-reported information from security-related survey questions that were asked as part of the underwriting process. Because cybersecurity-relevant information is either excluded for the premium pricing calculation or included to only a limited degree (Romanosky et al., 2017), the likelihood of cyber insurance being a primary driver for improving cybersecurity is an open question.

As discussed in Khalili, Liu, and Romanosky (2018), cyber insurers are just as risk averse as cyber insurance buyers and try to minimize their cost. Therefore, the challenge with pricing premiums at the optimal level in a manner commensurate with the underwritten risk is related to the insurer's ability to (1) assess and differentiate individual entity risk, as well as systemic or correlated risk, and (2) estimate losses for the full portfolio of policies and policyholders.

Considering existing data and methodological limitations, it would be logical to expect that insurers would be conservative in how they define the policies and pursue underwriting. As recently as 2016, there was evidence from cyber insurance market surveys that demand exceeded supply. However, that no longer appears to be the case, as the cyber insurance market has been experiencing an annual take-up rate of 25 to 30 percent in 2017 and 2018 (CIAB, 2018). The most recent market surveys show that insurers were reducing premiums and retentions, with coverage terms expanding and limits increasing (Advisen and PartnerRe, 2018; Betterley, 2017; CIAB, 2016a, 2016b, 2017, 2018; Marsh, 2018; Marsh Global Analytics Group, personal communication, 2018; PwC, 2018a).

Current market dynamics in cyber insurance do not seem to align with a practice of tight underwriting observed in more mature market segments (e.g., property and casualties under flood insurance programs). The latter follows mature guidelines based on robust and validated risk models, which are calibrated to abundant historical data and validated on a continuous basis. In contrast, the current cyber insurance market trends and practices indicate significant excess capacity, as evidenced by tight competition in underwriting and dropping premiums despite the high uncertainty with loss modeling.

The adverse implication of such market dynamics is that pricing for cyber insurance premium is based on judgment as opposed to closely modeled alignment with potential risks. If the underwriters derive their pricing decision from market pressure rather than evidence-based and model-derived assessment and subsequent differentiation of cyber risk levels, the perceived role of cyber insurance in advancing cybersecurity may be significantly limited.

Policy Coverage: Lack of Clarity, Coverage Overlaps, Coverage Specification, and Low Indemnity Limits

The language in cyber insurance policies is often unclear and ambiguous. This is in part due to the lack of a common lexicon or standardized policy language, a lack of consistency in the underwriting

process and forms, and variability in coverage and exclusions. These factors may be a result of how rapidly cyber risks evolve (CIAB, 2016a, 2016b, 2017, 2018; see Section 4.1.1). The unclear policies are often misinterpreted by decision makers, who may also mistakenly assume that cyber-related coverage is included under other policies they hold. It is also difficult for decision makers to determine what they want to be covered for due to the rapidly changing cyber threat environment. These are the are main reasons behind the low uptake in cyber insurance, particularly by small- and medium-sized businesses (A.M. Best, 2018b; CyRiE, personal communication, 2017; Marotta et al., 2017).

A natural question that arises is how the existing coverage in insurance policies compares with the type of loss that policy holders wish to indemnify. Romanosky et al. (2017) compared over 180 cyber insurance policies filed with state insurance commissions and found that existing policies have limited coverage and contain many exclusions.[9] It is a typical practice among insurers to set sublimits even within the cost and loss categories explicitly covered under the policies (CyRiE, personal communication, 2017; Marotta et al., 2017; Romanosky et al., 2017). The current types of coverage and low indemnity limits result in coverage gaps: that is, insurance policies only cover a small portion of losses incurred by organizations due to cyber incidents (Shetty et al., 2018). The gaps that concern insurance customers the most are security, loss prevention, risk control, business interruption, and remediation ("How Commercial Insurance," 2017).

As stated by A.M. Best (2018b), the limits for cyber policies are rather low in comparison with the traditional and better-understood policies such as property catastrophe risk. Low limits and sublimits for cyber policies are used as a means to avoid significant individual company losses and to manage accumulation risk. This is not a surprising outcome, as it is a direct consequence of the difficulty in predicting impact and effectively assessing the risks. The CIAB (2018) survey reports a decrease in the average policy limit from about $5 million in 2017 to $3.2 million. As reported by 80 percent of the brokers in CIAB, typical limits were below $5 million. The indemnity limits are too low in particular for large organizations, considering the difference in the potential scale of losses (Marotta et al., 2017).[10]

However, according to PwC (2018a), the market is soft, with capacity exceeding demand, premium pricing decreasing, and overall coverage limits increasing. In addition, sublimits such as contingent business interruption are either increasing or being eliminated from the policies. The Marsh (2018) Global Market Insurance Index third-quarter update states that business interruption has become a preeminent cyber risk. The Marsh Global Analytics Group (personal communication, 2018) analytics show overall increases in policy limits and coverage as well as persistent reductions in the price premiums per million of limits.

Legal Questions Regarding Liability and Compensation Practices

In addition to the factors described above that complicate cyber insurance purchasing decisions by potential customers, there are legal questions that cause significant difficulties with exercising claims and determining payout. With cyber insurance, it is difficult to determine who is liable for

[9] For more details on the content of cyber insurance policies, refer to the Romanosky et al. (2017) article which provides an overview of policy coverage, exclusions, triggers, conditions, and limits.

[10] As an example, Marotta et al. (2017) state that a maximum indemnity limit of $200 million would be too low for corporations such as Google.

an incident even if one could determine causality (CyRiE, personal communication, 2017; Marotta et al., 2017). Legal questions regarding liability and compensation practices present an additional source of uncertainty, and therefore, risk to both policyholders and insurers.

Moreover, the legal and regulatory environment surrounding liability and compensation practices is changing and varies by jurisdiction, which has financial implications for insurers (OECD, 2018). For example, insurance is regulated by states and there are 47 unique data breach notification laws at the state level (CIAB, 2018).

4.1.3. Summary

Risk-averse organizations participate in the cyber insurance market because they seek to transfer risk from cyber threats. However, there are multiple issues limiting the potential of the cyber insurance market and the pace at which the market is evolving. Cyber insurance is a new and specialized market with significant risks and difficulties for underwriting (PwC, 2018a) due to challenges presented by a lack of data, methodological limitations, and a lack of information sharing. These core challenges make it difficult for insurance companies to underwrite the risk at the right price. To do so, insurance companies would need underwriting guidelines, a risk management process, and robust and reliable pricing models that are continuously validated, especially given the dynamic nature of cyber risk.

In order for insurance companies to develop more mature cyber risk pricing models, they need data, time, and investment. However, insurers allocate less than 1 percent of their premium to cyber with the rest going to the traditional commercial insurance product lines with better understood risks and losses (A.M. Best, 2018b). Furthermore, insurance companies are cutting costs across the insurance industry. PwC (2018b) found that over 75 percent of insurers have implemented cost-cutting measures over the last 3 years and 61 percent of chief executive officers of insurance companies plan to launch cost reduction programs in 2018. Cost-cutting measures include gathering less information during the underwriting process, eliminating data fields in the notification of loss, cutting features and services, and removing coverage options to simplify billing and claims management.[11]

Given the data-sparse environment of cyber insurance, these cost-cutting trends may put a constraint on the investment and data collection that insurance companies would need to develop more mature and validated cyber loss models to properly align underwritten risk with price premiums. In addition, this trend runs counter to the expectation and recommendations of cyber practitioners that cyber insurers should be getting more involved with risk mitigation and reduction (PwC, 2018a).

Given the information asymmetry that exists between insurance companies and policyholders (see Section 4.1.1), it would be difficult for cyber insurers to get more involved risk mitigation and reduction. Policyholders have information on their respective security postures and vulnerabilities, while the insurance companies must rely on self-reported information from the policyholders to the extent that information is collected during the underwriting process.

[11] The notice of loss is the report filed by the policyholder with the insurance provider. It is the first step in the insurance claim lifecycle.

If the cyber insurance industry were to take on the role of a cybersecurity consultant, they would need to:

- possess more conclusive data on the effectiveness of cybersecurity controls and practices,[12]
- acquire and maintain a level of technical knowledge and expertise to advise on control selection and implementation conditioned on specific entity's security posture,[13] and
- maintain trade space analysis (i.e., information about the constantly evolving cyber technologies and solutions from vendors to understand which products provide the necessary level of functionality while meeting the cybersecurity requirements).

CIAB (2018) assessed that there is a trend of insurance companies partnering with cybersecurity organizations to quantify risk and provide post-event response and consulting. While this is a positive trend, those partnerships are predominantly utilized for post-event response and consulting rather than proactively advising on cybersecurity measures with preventative value or detection and protection capabilities. In addition, like insurance companies, cybersecurity organizations grapple with a lack of (1) historical loss data; (2) calibrated and validated risk quantification models; and (3) empirical evidence on the effectiveness of controls, processes, and practices to minimize the likelihood of an event occurring, or to minimize the consequences of such events. That is, the core challenges outlined by OCE in Section 4.1.1 are not specific to the cyber insurance market—they represent a broader set of challenges endemic to the entire cybersecurity industry.

4.2. Expected Impact of a Well-Developed Cyber Insurance Market

Insurance is a recognized mechanism for risk transfer, but can a well-developed cyber insurance market improve cybersecurity? This section evaluates the relationship between cyber insurance and cybersecurity, and the potential role the cyber insurance market can play in influencing cybersecurity.

A positive relationship between cyber insurance and a potential improvement in cybersecurity is increasingly becoming a commonly held hypothesis (CIAB, 2017, 2018; Romanosky et al., 2017; PwC, 2018a). However, rarely cited is empirical evidence supporting a pattern of association between cyber insurance and organizations improving cybersecurity practices and investing in controls to protect their networks, thereby increasing cybersecurity. Therefore, to better inform policy recommendations with respect to the potential for interventions and incentives to accelerate the maturation of the cyber insurance market, it is worth taking a critical look at lessons learned from other industries and insurance domains.

This section explores the evidence on whether insurance—as opposed to other driving factors such as regulatory requirements or legal action—has a strong and positive influence on the improvement of cybersecurity practices. It also offers suggestions for further research to explore and more conclusively determine whether this is indeed the case.

According to A.M. Best (2018b), the "US cyber insurance market took off as data breach notice and other privacy laws were implemented, which highlights the tangible costs associated with data

[12] For more information on controls, refer to the Center for Internet Security (2018) and Spacey (2016).

[13] For more information, refer to Rutherford (2018).

breaches" (p. 77). The cyber insurance market evolved as organizations became aware of the realized and tangible losses and there was more willingness to protect against those losses. The awareness came as a result of the regulatory imposition of fines for non-compliance, the reporting requirements, or legal action which made the losses realized and tangible.

This logic seems to serve as a foundation for the rational expectation that cybersecurity investment will be made to improve the defenses and cybersecurity posture in exchange for reductions in premiums for comparable coverage or higher liability limits (CIAB, 2016a, 2016b, 2017, 2018; Pal, 2012). Academic literature, specifically the theoretical modeling literature on cyber insurance markets, also shows that (1) cyber insurance can increase collective cybersecurity because policyholders increase self-defense in response to increases in premiums (Pal, 2012; Kesan, Majuca, & Yurcik, 2004, 2005), and (2) it is a useful complement to other cybersecurity measures (Pal, 2012; Lelarge & Bolot, 2008, 2009).

However, as the CIAB (2018) survey notes, although the most recent regulations in the European Union and the United States as well as coverage of the latest cyberattacks have increased awareness of cyber risks, it did not result in a significant increase in purchased cyber coverage, even though prices stayed the same or decreased.[14] Of the respondents, 37 percent and 49 percent indicated that new regulations had no impact, or only somewhat of an impact, on their coverage purchasing practices, respectively. When asked about the impact of recent cyber events, almost a third indicated there was an effect on their decision, while half indicated only somewhat of an impact. The remaining 20 percent cited no impact. This could be partially explained by a lag in purchasing behavior in response to the regulations, as they only recently went into effect. However, they were announced long before going into effect; therefore, the market had a few years to form an expectation and respond accordingly. Another possible explanation is that although the regulations are in effect, given the lack of precedent, there was little anticipation of fines under those new regulations when the survey was administered, which made the decision makers discount that risk.

Furthermore, because of the extremely competitive market, "insurers were reducing premiums and retentions if pushed with competition. Coverage terms also continued to expand" (CIAB, 2018, p. 5). This implies that premiums are currently more sensitive to the competitive pressure in the market rather than the security posture and perceived threat, and ultimately, than the marginal differences in the potential cyber risk between policyholders.

Moreover, CIAB (2018) shows that a majority of brokers did not see increased scrutiny from carriers with respect to underwriting, even with the elevated awareness resulting from the most recent breaches. This challenges the premise that insurance can improve cybersecurity standards and best practices by requiring a minimum level of security as a pre-condition or basing a premium on the security posture of the policyholder. At a minimum, it requires (1) a body of knowledge, conclusive evidence, and consensus as to what could constitute a minimal level of security; and (2) an empirical basis for correlating deployed controls or overall security posture above that

[14] The European Union approved the General Data Protection Regulation in 2016. This regulation went into force in May 2018 and establishes a "set of data protection rules for all companies operating in the EU" (European Commission, 2018, Background section, para. 1). The New York State Department of Financial Services approved the cybersecurity requirements for financial services companies in March 2017. This regulation went into force in August 2017 and "requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion" (N.Y. Comp. Codes R. & Regs, p. 1).

minimum level with positive or negative outcomes. Neither of these elements is sufficiently evolved to support such an approach to underwriting. Given the soft market, differences in premiums would have a limited ability to improve cybersecurity while there is excess capacity, and especially naïve capacity, in the cyber insurance market (Smith, 2018).

References

Advisen and PartnerRe. (2018). 2018 survey of cyber insurance market trends. Retrieved from https://partnerre.com/wp-content/uploads/2018/10/2018-Survey-of-Cyber-Insurance-Market-Trends.pdf

AIR Worldwide develops probabilistic model for global cyber risks. (2018, October 22). *Insurance Journal*. Retrieved from https://www.insurancejournal.com/news/national/2018/10/22/505209.htm

Akerlof, G. (1970). The market for lemons: Qualitative uncertainty and the market mechanism. *Quarterly Journal of Economics*, *84*(3). 488–500. doi:10.2307/1879431

A.M. Best (2018a). A.M. Best report examines cyber insurance. *Best's Review*, *7*, 79–80.

A.M. Best (2018b). Special report focuses on cyber insurance. *Best's Review*, *10*, 76–77.

Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society*, *367*(1898), 2717–2727. doi:10.1098/rsta.2009.0027

Aon Inpoint. (2017). *Global cyber market overview: Uncovering the hidden opportunities*. Retrieved from http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf

Bermuda:Re+ILS. (2018, December 7). Cyber: Still small for its age. *Bermuda Insurance Magazine*. Retrieved from https://www.bermudareinsurancemagazine.com/ contributed-article/cyber-still-small-for-its-age

Betterley Risk Consultants, Inc. (2017). The Betterley Report: Cyber/Privacy insurance market survey—2017. Retrieved from https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf

Business Wire. (2018). Best's special report: Cyber insurance market sees steady growth but still awaiting a real growth spurt. Retrieved from https://www.businesswire.com /news/home/20180521005631/en/Best%E2%80%99s-Special-Report-Cyber-Insurance-Market-Sees

Center for Internet Security. (2018). CIS Controls™ FAQ. Retrieved from https://www.cisecurity.org/controls/cis-controls-faq/

The Council of Insurance Agents & Brokers. (2016a). *Cyber insurance market watch survey: Executive summary*. Retrieved from https://www.ciab.com/wp-content/uploads/2017/04/102016CyberSurvey_Final.pdf

The Council of Insurance Agents & Brokers. (2016b). *Cyber insurance market watch survey: Executive summary*. Retrieved from https://www.ciab.com/wp-content/uploads/2017/04/2ndCyberMarketWatch_ExecutiveSummary_FINAL.pdf

The Council of Insurance Agents & Brokers. (2017). *Cyber insurance market watch survey: Executive summary*. Retrieved from https://www.ciab.com/wp-content/uploads/2017/05/Spring2017_CyberSurvey_ExecSummary_FINAL.pdf

The Council of Insurance Agents & Brokers. (2018). *Summer 2018 cyber market watch survey highlights*. Retrieved from https://www.ciab.com/resources/summer-2018-cyber-market-watch-survey-highlights/

Cyber Risk Economics Research. (2018). Cyber Risk Economics capability gaps research strategy. Retrieved from Department of Homeland Security, Science and Technology website: https://www.dhs.gov/sites/default/files/publications/ 3950_CYRIE_Report_FINAL508.pdf

Day, J. (2018, June 12). Challenging the economics of cybersecurity with cyber threat intelligence-sharing programs: Part 2 [Web log post]. Retrieved from https://www.lookingglasscyber.com/blog/challenging-the-economics-of-cybersecurity-with-cyber-threat-intelligence-sharing-programs-part-2/

de Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 239–274. doi:10.1057/s41288-018-0082-7

Eling, M. & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474–491. doi:10.1108/JRF-09-2016-0122

European Commission. (2018). 2018 reform of EU data protection rules. Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Hern, A. (2017, December 30). WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017. *The Guardian*. Retrieved from https://www.theguardian.com/ technology/2017/dec/30/wannacry-petya-notpetya-ransomware

How commercial insurance customers rate large carriers, brokers. (2017, December 7). *Insurance Journal*. Retrieved from https://www.insurancejournal.com/news/national/ 2017/12/07/473440.htm

J.D. Power. (2017, December 4). Diversity of offerings becomes key differentiator for larger commercial insurers, J.D. Power find. Retrieved from https://www.jdpower.com/ business/ press-releases/jd-power-2017-large-commercial-insurance-study

Kesan, J., Majuca, R., & Yurcik, W. J. (2004). The economic case for cyberinsurance (Illinois Law and Economics Working Paper Series No. LE04-004).

Kesan, J., Majuca, R., & Yurcik, W. J. (2005). *Cyberinsurance as a market-based solution to the problem of cybersecurity: A case study*. Paper presented at the Fourth Workshop on the Economics of Information Security, Cambridge, MA. Retrieved from https://pdfs.semanticscholar.org/fbac/ fbf013bae9077165280e1da04438d0b0c1d8.pdf

Khalili, M. M., Liu, M., & Romanosky, S. (2018). Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Proceedings of the 17th Workshop on the Economics of Information Security (WEIS 2018).*

Kunreuther, H. & Heal, G. (2003). Interdependent security. *The Journal of Risk and Uncertainty, 26*(2/3), 231–249. doi:10.1023/A:1024119208153

Lelarge, M. & Bolot, J. (2008). *Cyber insurance as an incentive for internet security*. Paper presented at the Seventh Workshop on the Economics of Information Security, Hanover, NH. Retrieved from https://www.econinfosec.org/archive/weis2008/papers/ Lelarge.pdf

Lelarge, M. & Bolot, J. (2009). Economic incentives to increase security in the internet: The case for insurance. *2009 Proceedings IEEE INFOCOM*. 1494–1502.

Ligon, J. & Thistle, P. (1996). Information asymmetries and informational incentives in monopolistic insurance markets. *The Journal of Risk and Insurance, 63,* 434–459. doi: 10.2307/253620.

Marotta, A. Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61. doi:10.1016/ j.cosrev.2017.01.001

Marsh. (2018). *Global Market Insurance Index: Third quarter 2018.* Retrieved from https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/GIMI-Q3-2018.pdf

NetDiligence. (2018a). *2018 cyber claims study*. Retrieved from https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf

NetDiligence. (2018b). Welcome to the eRiskHub®. Retrieved from https://eriskhub.com/

N.Y. Comp. Codes R. & Regs. Tit. 23, § 500

Organisation for Economic Co-operation and Development. (2018). *Unleashing the potential of the cyber insurance market: Programme*. Retrieved from https://www.oecd.org/daf/fin/insurance/Unleashing-the-potential-of-the-cyber-insurance-market-final-programme.pdf

Pal, R. (2012). Cyber-insurance in internet security: A dig into the information asymmetry problem. *The Computing Research Repository*. 1–6.

PwC. (2018a). *Are insurers adequately balancing risk & opportunity? Findings from PwC's global cyber insurance survey*. Retrieved from https://www.pwc.com/us/en/industry/ assets/pwc-cyber-insurance-survey.pdf

PwC. (2018b). *Top issues: Shifting cost curves to stay in the commercial insurance race*. Retrieved from https://www.pwc.se/sv/pdf-reports/forsakring/insurance-top-issues-2018-commercial-cost-curve.pdf

Risk Management Solutions, Inc. (2016). Managing cyber insurance accumulation risk. Prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge. Retrieved from https://www.jbs.cam.ac.uk/ fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). *Content analysis of cyber insurance policies*. Working paper retrieved from RAND website: https://www.rand.org/pubs/working_papers/WR1208.html

Rutherford, S. (2018). What is a cybersecurity posture? [Web log post]. Retrieved from FICO website: https://www.fico.com/blogs/fraud-security/what-is-a-cybersecurity-posture/

Shetty, S., McShane, M., Zhang, L., Kesan, J. P, Kamhoua, C. A, Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 224–238. doi:10.1057/s41288-018-0078-3

Smith, R. (2018, May 11). Cyber insurance market continues to accelerate. Retrieved from Insurance Business America website: https://www.insurancebusinessmag.com/us/news/cyber/cyber-insurance-market-continues-to-accelerate-100346.aspx

Spacey, J. (2016, December 10). 11 examples of security Controls. Retrieved from Simplicable website: https://simplicable.com/new/it-security-controls

U.S. Securities and Exchange Commission, Division of Corporation Finance. (2011). CF disclosure guidance: Topic no. 2: Cybersecurity. Retrieved from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Verizon (2018). *2018 Data breach investigations report.* Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Appendix A – Suggestions for Further Research

If more time is allowed to pursue the subject, the following activities could further refine the market assessment through collection of additional secondary and primary sources:

- Conduct a more detailed comparative analysis to establish empirical evidence if insurance resulted in individual and group behavioral changes that permanently improved the collective state of a system in other, more mature sectors.
- Review current efforts by the insurance and cybersecurity companies to partner up in offering bundled services that include cyber risk scoring, cyber security technical assistance or consultancy, predictive cyber risk modeling and cyber insurance (Kovrr, Konfidas, etc).
- Review current efforts in streamlining cyber insurance language, coverage and risk modeling, and establish relationship with the Geneva Association, the leading international think tank consisting of 90 insurance and reinsurance CEOs, and their affiliated organizations (European Bank of Risk and Insurance Economists, Annual Round Table of Chief Risk Officers, Cyber Risk Office Assembly, Annual Circle of Chief Economists, etc), as well as foreign governments already successfully collaborating with the cyber insurance industry (e.g., Israel).
- Analyze if insurance markets in other domains successfully evolved on their own or if government regulations and requirements and the legal environment were the driving force for maturation.
- Review lessons learned from other industries with required liability insurance to understand if making cyber insurance mandatory (akin to federal flood insurance in high-risk flood areas or medical insurance for health practitioners), has a sufficient impact on advancing the state of the entire system or network.
- Review lessons about disclosures of events and losses from other sectors such as medical and auto insurance.
- Analyze if the Federal Energy Regulatory Commission model on reporting events could affect reliability (as opposed to having tangible material consequences) and if it could be adapted to improve the reporting and disclosure of cyber incidents.

Appendix B – DHS Activities in Addressing Cyber Insurance

Recognizing the need to accelerate the development of the cyber insurance market, DHS has undertaken several initiatives in this space. DHS S&T has being funding two programs that explore the gaps and advance the research and implementation. The first one, CyRiE, explicitly prioritizes the role of insurance as one of its key research areas and aims to study how existing product liability frameworks may be applied to address cybersecurity failures in the context of increasingly connected networks and devices.

As part of its programmatic activities, CyRiE conducts regular stakeholder exchange meetings (SEMs) where participants representing the government, private sector, and academia discuss existing challenges and potential solutions. The analysis in this paper draws on some of the gaps, challenges, and obstacles in the cyber insurance market that were identified by the stakeholders as part of the CyRiE SEMs in fiscal years 2017 and 2018.

CIRI also conducted research on cyber insurance. CIRI is a DHS Center of Excellence led by the University of Illinois at Urbana-Champaign, funded by the Office of University Programs at DHS S&T. Their most recent publications on the topic of the cyber insurance market and the level of its maturity also served as the basis for the analysis in this paper.

The third effort undertaken by DHS is the Cyber Incident Data and Analysis Work Group/CIDAR project. The project intended to bring together researchers, cybersecurity practitioners, and cyber insurance stakeholders as part of collaborative effort to promote the exchange of cyber incident data. The project culminated in the publication of three sets of meeting proceedings that identified data sharing challenges, as well as notional data points that could potentially support the analysis, if shared voluntarily by cyber insurance carriers and cybersecurity practitioners.

Subsequent efforts from the work group were focused on refining the initial set of data points to reduce the reporting burden on potential data contributors. The project faced the same challenges as private sector initiatives in this space, as a result the prototype repository has not been established and no data have been gathered. However, key obstacles to the development of the cyber insurance market and issues with cyber incident data sharing identified by the work group remain unresolved, and as such, are also incorporated in this analysis.