Working Paper

Content Analysis of Cyber Insurance Policies

How do carriers write policies and price cyber risk?

Sasha Romanosky, Lillian Ablon, Andreas Kuehn, Therese Jones

RAND Justice, Infrastructure, and Environment

WR-1208
September 2017

For more information on this publication, visit www.rand.org/pubs/working_papers/WR1208.html

Published by the RAND Corporation, Santa Monica, Calif.

Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk?

Sasha Romanosky, sromanos@rand.org*
Lillian Ablon, lablon@rand.org
Andreas Kuehn, akuehn@rand.org
Therese Jones, tjones@rand.org

Abstract

Data breaches and security incidents have become commonplace, with thousands occurring each year and some costing hundreds of millions of dollars. Consequently, the market for insuring against these losses (aka cyber insurance) has grown rapidly in the past decade. However, very little is known about these policies and the mechanisms behind the risk assessments. While there exists much theoretical literature about cyber insurance, very little practical information is publicly available. For example, what losses are actually covered by cyber insurance policies, and what are the exclusions? What factors are used to compute the premiums, and how do existing underwriting approaches reflect the technical rate of risk? In this research, we collect and analyze over 180 cyber insurance policies filed with state insurance commissioners. By analyzing these policies, we provide the first-ever analysis of the underwriting process for cyber insurance and uncover how insurance companies understand and price cyber risks.

Keywords: cyber insurance, cyber liability, pricing cyber risk

Acknowledgments: We would like to thank Adam Hamm, Igor Mikolic-Torreira, Elizabeth L. Petrun Sayers, Lori Uscher-Pines, participants of the 2017 Workshop on the Economics of Information Security (WEIS) and the 2017 Research Conference on Communications, Information and Internet Policy (TPRC). We would also like to thank RAND's Institute for Civil Justice, and the William and Flora Hewlett Foundation for their generous support.

* Corresponding author

Introduction

Cyber insurance is a broad term for insurance policies that address first and third party losses as a result of a computer-based attack or malfunction of a firm's information technology systems. For example, one carrier's policy defines computer attacks as, "A hacking event or other instance of an unauthorized person gaining access to the computer system, [an] attack against the system by a virus or other malware, or [a] denial of service attack against the insured's system."[1]

Despite the strong growth of the cyber insurance market over the past decade, insurance carriers are still faced with a number of key challenges: how to develop competitive policies that cover common losses, but also exclude risky events?; how to assess the variation in risks across potential insureds; and how to translate this variation into an appropriate pricing schedule?

Since insurance in the US is regulated at the state level, insurance carriers are required to file notices to state insurance commissions describing each new insurance product. These filings include the full text of the policy (coverage, exclusions, triggers, etc.), a security application questionnaire, and a rate schedule describing the formula for deriving insurance premiums. It is these filings that provide a unique opportunity to examine how insurance companies understand and price risks, and specifically, which business, technology and process controls (if any) are considered in rate calculations.

In this research paper, we seek to answer fundamental questions concerning the current state of the cyber insurance market. Specifically, by collecting over 180 insurance policies from state insurance commissions across New York, Pennsylvania, and California, we examine the composition and variation across three primary components:

- The coverage and exclusions of first and third party losses which define what is and is not covered,
- The security application questionnaires which are used to help assess an applicant's security posture, and
- The rate schedules which define the algorithms used to compute premiums.

Overall, our research shows a much greater consistency among loss coverage and exclusions of insurance policies than is often assumed. For example, after examining only 6 policies, 88% of the coverage topics had been identified, while only 52% of all exclusions were documented. However, while each policy may include commonly covered losses or exclusions, there was often additional language further describing exceptions, conditions, or limits to the coverage.

The application questionnaires provide insights into the security technologies and management practices that are (or are not) examined by carriers. For example, our analysis identified four main topic areas: Organizational, Technical, Policies and Procedures, and Legal and Compliance. Despite these sometimes lengthy questionnaires, however, there still appeared to be relevant gaps. For instance, information about the security posture of third-party service and supply chain providers and are notoriously difficult to assess properly (despite numerous breaches occurring from such compromise).

In regard to the rate schedules, we found a surprising variation in the sophistication of the equations and metrics used to price premiums. Many policies examined used a very simple, flat rate pricing (based simply on expected loss), while others incorporated more parameters such as the firm's asset value (or firm revenue), or standard insurance metrics (e.g. limits, retention, coinsurance), and industry type. More sophisticated policies then incorporated information security controls and practices, sometimes collected from the security questionnaires.

[1] POL-35. Note that we will obfuscate the actual policy numbers and companies throughout this manuscript.

By examining these components of insurance contracts, we hope to provide the first-ever insights into how insurance carriers understand and price cyber risks.

Supply and Demand for Cyber Insurance

The U.S. cyber insurance market has been growing rapidly over the past decade. With less than $1 billion in premium in 2012, some experts estimate that the US cyber insurance market will grow to $7.5 billion by the end of the decade (PwC, 2015), with others projecting $20 billion by 2020 (Hemenway, 2015).

The North America cyber insurance market accounted for around 90% of the global cyber insurance market in 2015 (Allied Market Research, 2016; PwC, 2015), which provides significant growth opportunities for the cyber insurance market on the international level. Estimated compound annual growth rates for this market have been reported to range between 28% and 37% (Hemenway, 2015; PwC, 2015) and a recent survey of industry leaders found that 88% of respondents saw cyber as a "potentially huge untapped market" which they anticipated would grow faster than the rest of the property/casualty (P/C) insurance industry (Insurance Information Institute, 2017).

While the U.S. market penetration may be more advanced than other countries, only around one third of US companies have purchased some sort of cyber insurance (Aon Benfield, 2014), with significant variation in cyber insurance across U.S. industry sectors. For example, barely 5% of manufacturing firms have cyber insurance coverage, whereas the healthcare, technology and retail sectors have reached an adoption of close to 50% (Willis, 2014).[2] In the UK, this number drops to only 2% for large firms with cyber insurance (UK Cabinet Office, 2015). Yet, Marsh (2016) reports cyber insurance growth rates of 27% across all industries, ranging from 6% in health care to 63% in manufacturing, for U.S.-based clients in 2015.

The supply side of insurance is also growing very rapidly. While only a few firms were offering insurance products, the National Association of Insurance Commissioners (NAIC) reported there to be around 500 carriers now offering cyber insurance to businesses and individuals (NAIC, 2016). That being said, reports suggest that the U.S. cyber insurance market is dominated by a handful of carriers, including: American International Group, Inc. (AIG), accounting for approximately 22% of the market, Chubb Limited (CB) at 12%, and XL Group Ltd. (XL) at 11% (Fitch Ratings, 2016), with ACE Ltd, Zurich and Beazley also providing much coverage.

While the cyber insurance market has grown considerably since the early 2000s, compared to the overall insurance market, cyber remains a small component of overall corporate insurance. As of 2015, premiums in the commercial insurance market were $247 billion, compared to the estimated $2 billion for cyber insurance (thus representing less than 1%), offered by close to 6000 insurance firms (Insurance Information Institute, n.d.-a, n.d.-b). And relative to the cybersecurity market, Gartner estimated the 2015 worldwide cybersecurity market at $75.4 billion, and forecasted to grow to $170 billion by 2020 (Morgan, 2015).

Average premiums are priced between $10,000 and $25,000,[3] with some carriers writing limits between $10 million and $25 million, and as high as $50 million (Betterley, 2012). Other reports suggest typical

[2] Marsh (2015) also reports an adoption rate of 16% across all industries; 8% in manufacturing; 50% in health care, but lower adoption numbers of 12% in communications, media, and technology, and 18% in retail/wholesale – for clients purchasing standalone cyber insurance in 2014.

[3] Personal correspondence with an executive of a large insurance carrier.

premiums of $100,000 for limits of $10 million (Airmic, 2012). While deductibles (aka retention) may be as low as $5,000, deductibles between $500,000 and $1 million are common for companies with $1 billion or more in assets, with some reaching as high as $25 million.[4]

One carrier stated that average limits increased by 20% to $16.8 million, relative to 2011 (Marsh, 2013). driven by communications, media, and technology companies and induced through federal regulation, such as HIPAA, and data breach disclosure laws. As with most other insurance products, towers of cyber policies can be purchased in the event of extreme losses, and Airmic (2012) suggests that limits of $200 million and $300 million exist for some industries. As of 2015, most large towers comprise between $200 million and $400 million in limits (Marsh, 2016).

Coverage for cyber insurance may be stand-alone, or provided as an endorsement (amendment) to another policy. Cyber coverage as endorsements is often written to E&O ("errors and omissions") policies.[5] In one survey, 60% of carriers provided cyber insurance through both stand-alone policies and endorsements, while around 33% provided only stand-alone (Partner Re and Advisen, 2016). Since the Federal Insurance Office recently announced a government backstop for standalone cyber insurance policies under the Terrorism Risk Insurance Act of 2002, it is expected that U.S. cyber insurance policies will increasingly be written as standalone policies.[6]

How is Cyber Insurance Regulated?

In the United Sates, insurance laws are statutorily enforced by the McCarran–Ferguson Act (15 U.S.C. §§ 1011-1015) which empowers states to regulate the "business of insurance," and which is overseen by a non-profit organization called the National Association of Insurance Commissioners (NAIC), which helps coordinate insurance policies across the states. State laws require that all insurers, agents, and brokers, must be licensed to sell insurance; that the products they provide are understood by consumers without any obfuscated gaps in coverage or terms; and that the rates to be charged are not "excessive, inadequate, or unfairly discriminatory."[7] *Excessive* implies that the premiums are not priced unreasonably high, *adequacy* implies that the premiums are high enough in order to support the business for the carrier, and *discriminatory* implies that any price differences appropriately reflect variation in actual risk across firms.[8]

Despite this, product regulation, rating rules, and coverage requirements can vary state by state. For example, half of US states require rate approval for personal lines of coverage for property and casualty insurance. On the other hand, commercial lines enjoy a competitive rating system, under which states reserve the right to disapprove of rates if they deem competition to be unfair, but do not authorize rates in advance. In addition, health insurance is typically subject to rate approval, while almost all other lines of insurance, including life and annuity products, are not typically subject to review (NAIC, 2017).

Other differences relate to the rating approach of each state, and rating exemptions given to particular types of insurance. For example, in property/casualty insurance (of which cyber insurance relates), three major rating approaches are used: prior approval, file-and-use, and open competition (Baranoff, Brockett, and Kahane, 2009). In prior approval, an insurer requires permission of the state insurance commissioner prior to use. File-and-use is similar to prior approval, but allows immediate use of the rate until the commissioner's decision, usually made within a 30-day period. Open competition requires no rate filings

[4] Personal correspondence with an executive of a large insurance carrier.
[5] Personal correspondence with an executive of a large insurance carrier. Yet, a recent NAIC report also suggests that endorsements are written to commercial (CGL) or personal insurance policies (Nordman, 2016).
[6] Personal correspondence with an executive of a large insurance carrier. See also Kalinich (2017).
[7] This phrase is universal across state agencies and represents the spirit of state insurance regulation.
[8] See http://www.iii.org/issue-update/regulation-modernization.

(Baranoff, Brockett, and Kahane, 2009). Even states that require prior approval or file-and-use for property and casualty insurance may have specific markets that are exempt from filing; "computer fraud" is one such exemption for several states (NAIC, 2017).

In addition to rating requirements, states also impose financial regulation on all insurers. Financial examinations are scheduled by state regulatory authorities to verify accounting practices, procedures, and other information delivered in the company's annual statement. Failing this examination subjects the company to possible state takeover. The state also maintains a system that guarantees consumers' protection in the event of financial insolvency of the insurer. Similarly, market conduct examinations are performed on a regular basis by the state to ensure fair pricing and consumer protection. Such examinations may also be prompted by consumer complaints, received through state consumer protection hotlines and websites (NAIC, 2017).

Despite these variations, state regulations generally provide the same rules and procedures governing the filing, pricing and coordination of policies and rate schedules.

Admitted vs Non-Admitted Insurance Markets

An important distinction regarding insurance regulation concerns *admitted* versus *non-admitted* markets. Carriers that seek to operate in an admitted market must receive a license by the state insurance commission to sell insurance in that state, must comply with all state regulations, and file their policies and rate schedules with the state insurance departments. One advantage of this oversight for consumers is that it helps prevent abuse by insurance companies. In addition, admitted carriers pay into a guarantee fund, which is used to pay the insured in the event that an insurer becomes insolvent and unable to pay the claims of its insureds. This safety feature does not exist for non-admitted carriers, and as one may imagine, the bulk of personal auto and homeowner insurance is written by admitted carriers.

Carriers that operate in the non-admitted market (also known as excess and surplus insurance lines) are still able to operate in a given state, but are not bound by many of the regulations imposed on admitted carriers, and are not required to file their policies or rate schedules with the state insurance commissions. Ostensibly, this affords these carriers more flexibility to modify the policies or rates more quickly, and can be very useful when the risks of a new market and insureds are uncertain (Markel, 2017 and NAPLIA, 2013) Policies from non-admitted insurers are still purchased from state-licensed brokers, and licenses may be denied by the state if the management is deemed incompetent or unethical (Baranoff, Brockett, and Kahane, 2009). Some states even maintain lists of eligible surplus line insurers, or of surplus lines known to be unauthorized (Dearie Jr., 2015).

Some suggest that a sizeable portion of all cyber insurance policies fall under non-admitted markets. Indeed, one estimate suggests that this could be as high as 90% of the cyber insurance market. On the other hand, other experts state that cyber insurance is "moving rapidly into the [non-admitted] market for many industries and for smaller firms" and that "a lot of admitted markets are now providing some form of cyber cover" (Greenwald, 2016). Further, many non-admitted insurance companies are owned by admitted market insurance companies, for example, Chartis (Lexington) and Chubb each have non-admitted partners (Gardner, 2014).

Nevertheless, based on our preliminary analysis and discussion with industry experts, we find no reason to believe that there would be material differences in written policies between those of the admitted and non-admitted markets.

The Theory of Cyber Insurance

With few exceptions, the academic cyber insurance literature consists of strictly theoretical papers that examine the viability of cyber insurance markets (Johnson et al, 2011; Böhme and Schwartz, 2010a; Böhme, 2010b; Böhme and Kataria, 2006a; Böhme and Kataria, 2006b).[9] Overall, this body of literature examines the incentives for firms to purchase insurance (demand side), the incentives for insurers to provide contracts (supply side), and the conditions necessary in order for a market to exist. The inevitable tension for firms, as many identify, is whether to invest in ex ante security controls in order to reduce the probability of loss, or to transfer the risk (cost) to an insurer.

As the collective research describes, the defining characteristics of cyber insurance are *interdependent security*, *correlated failure*, and *information asymmetry*. Some of these properties are common to all insurance markets, while others -- and their combined effects -- are unique to the risks of networked computing systems and cyber insurance. First, interdependent security reflects the degree to which the security of one computer network is affected by the compromise of another system (the breached system is said to impose a negative externality on the victim). For example, the security of the DCA airport in Washington, D.C. may be compromised if luggage from SFO is not properly screened (Kunruther and Heal, 2003).

Second, correlated failure (also known as systemic risk), is the systematic failure of multiple, disparate systems due to a single event. Correlated failures may occur in multiple ways, such as from a single source (e.g. a criminal group attacking many businesses), failure of a single IT system upon which many businesses operate (e.g. cloud provider or virtualization data center), or compromise of many devices due to a common vulnerability or exploit (e.g. a distributed denial of service attack). (Notice the loss is further amplified by interdependent security.) Finally, information asymmetry in the context of insurance reflects the familiar moral hazard and adverse selection problems (i.e. companies behaving more risky when fully protected from loss; and insurance carriers not being able to differentiate between high and low risk clients).

It should be emphasized that while there are ways of reducing information asymmetries, *insurance carriers* are mainly concerned with correlated failures because it defines the degree to which a security breach by one firm affects another, and therefore any indemnities paid. On the other hand, *firms* are mainly concerned with interconnected nodes because this determines how a failure by a business partner may affect them. However, as Böhme and Schwartz (2010) point out, the commonality is interconnected computing systems.

Böhme & Schwartz (2010) provide an excellent summary of cyber insurance literature and define a unified model of cyber insurance that consists of 5 components: the networked environment, demand side, supply side, information structure, and organizational environment. First, the network topology plays a key role in affecting both interdependent security and correlated failures. i.e. consider the difference in impact between extremes of independent computers versus a fully connected computing network. Their demand-side models consider the risk aversion of the insured, heterogeneity across wealth, impact, and defense and utility functions of firms. The supply-side discussion considers, among other properties, the competitive landscape of insurers, contract design (premiums, fines), and the carrier's own risk aversion. Discussion of information structure relates to adverse selection and moral hazard. Finally, organizational environment describes issues such as regulatory forces that may exist to mandate insurance, require disclosure in the event of a loss, and the effect of outsourced security services and hardware and software vendors on a firm's security posture.

[9] This section appeared, in part, in Department of Commerce, Comments to Docket No 130206115-3115-01 1/10 by Sasha Romanosky, April 26, 2013.

As mentioned, risk management is often framed as a trade-off between investing in controls that reduce the average loss of a security event, and insuring against a loss. Indeed, Ehrlich and Becker (1972) show that as insurance becomes more affordable, there is less incentive to invest in self-protection (IT security) measures. At an extreme, if the price of insurance were very inexpensive, companies would be very unlikely to protect themselves against any kind of loss. Conversely, as insurance becomes more expensive, companies become more willing to self-protect (the price of insurance becomes much higher relative to any security measures). Ehrlich and Becker (1972) also suggest that the demand for insurance is increasing in the size of the loss, and decreasing in probability of loss. That is, companies are more willing to insure against larger, less frequent loss events.

Research Methodology

The goal of this research is to explore and describe the three main components of cyber insurance policies: coverage, applications, and rate schedules. In order conduct this analysis we conducted a directed content methodology which enables us to identify and categorize themes and concepts, and derive meaning and insights across policies.[10]

Determining the proper methodological approach requires addressing two primary considerations: the sampling strategy (i.e., which data to collect) and the analysis technique (i.e., how to analyze the policies we collect). For the first consideration, our primary goal is to devise a sampling strategy that allows us to describe the full range of policies and their characteristics in the U.S. For example, the best approach may come from selecting across states, carriers, industry lines of business, or something else.

Our previous discussion concerning state-level regulation, as well as conversations with industry experts and regulators, suggests that there would be no material variation across the states in the content of insurance policies. This is not to say that there should be no differences across states, but just none that would materially bias any results or conclusions. For example, it may be true that more populated states would enjoy more competition, and therefore contain more policies; there may be more variation in content within these larger states, relative to smaller states; and the policies, themselves, may be geared toward larger companies (i.e. larger limits). Nevertheless, the lack of *material* differences across state regulations suggest that, for the purpose of data collection, we could reasonably consider all US states to be similar, thus supporting a pooled analysis.

For the purpose of this research, we estimate the size of the full population of cyber insurance policies to be around 2000-3000, a number larger than this research effort is able to examine.[11] Therefore, our data collection began by downloading policies from New York, Pennsylvania, and California. These states were chosen as preliminary data sources because they are three of the largest states by population, and where we therefore expect to see a large number of policies, with more variation.

In order to determine the appropriate number of policies to examine, we leverage a form of qualitative non-probabilistic sampling known as *purposive sampling*. Sample size in purposive sampling methodologies is determined by a concept called *saturation*, which is the point at which "no additional data are being found whereby the (researcher) can develop properties of the category. As [the researcher] sees similar instances over and over again, [she] becomes empirically confident that a category is saturated" (Glaser and Strauss, 1967). Guest (2006) further defines (theoretical) saturation as the "point in data collection and analysis when new information produces little or no change to the codebook" while at the same time, the observations are "selected according to predetermined criteria relevant to a particular

[10] This approach differs from a summative analysis where one would already have an exhaustive list of appropriate keywords and focus on the use of specific terms of interest and how common they are as compared to other terms.
[11] This estimate is based on extrapolating based on the total number from a small sample of states.

research objective" (Guest, 2006) – such as in our case of studying cyber insurance coverage from a larger pool of all state insurance. Specifically, Guest (2006) states that "the size of purposive samples be established inductively and sampling continue until 'theoretical saturation' (often vaguely defined) occurs" (Guest, 2006).

As mentioned, our content analysis consists of three parts: the coverage, security applications, and rate schedules. Meta data concerning each insurance policy (such as the date filed, insurance line, policy name, etc.) was first coded. Two coders were then assigned to examine the coverage section, and one coder was each assigned to the security application, and rate schedule sections. Each coder developed their own code book as they examined and processed a document.

The code books enumerated and tracked the content areas that were relevant to each section of the cyber insurance policy. For example, the code book for the policy coverage section identifies which losses are covered or excluded by the policy; the code book for the security questionnaire section defined which question each policy asked; and similarly with the rate schedule code book. The research team also met to review and validate the codebooks. We first applied a deductive approach to anticipate initial coding variables, which were then updated based on analysis of the content in real time to capture unexpected findings, creating new (or collapsing redundant) themes, as needed. Coding is further described within each section.

As will be described, coding is based on objective measures of observed content within the each of the sections of the insurance policies, rather than other content which may be highly subjective and therefore more susceptible to inter-rater reliability or measurement error. For example, coding was based on the presence/absence of content such as which losses were covered (objective), as opposed to coding for degree of negative sentiment in the language of a policy (subjective).

Data

Our primary source of data collection comes from the SERFF Filing Access system, an online electronic records system managed by the National Association of Insurance Commissioners (NAIC). SERFF was developed by NAIC in the 1990s in order to facilitate the "submission, review and approval of product filings between regulators and insurance companies."[12] The documents filed include the policy forms (description of coverage, triggers and exclusions), application forms (the self-assessment questionnaires presented to clients in order to assess their security posture), rate information (equations and tables governing the pricing of premiums), and any supporting documentation required or requested by the state insurance commissioners. As of 2016, 49 states and 3900 insurance companies and filers all participate with SERFF (though not all states allow electronic filing). Further, the adoption of this electronic filing system by multiple states ensures uniformity and consistency of filed documents across all states. These documents are made available to the public in part, due to state open records laws.[13]

Our search strategy consisted of searching for policies from specific US states using the keywords: "cyber," "security," and "privacy" and searching only property and casualty lines of insurance. We collected the most current and *approved* documents including the coverage forms, rates and rules

[12] See http://www.serff.com/about.htm, last accessed January 20, 2017

[13] Most often, the actual documents are filed by underwriting analysts employed by the carrier, or outsourced to specialized firms, or third parties agents, filing on behalf of the carrier. For example, we found a number of instances where insurance carriers employ the services of a third party organization which developed model policies and premium rates. In effect, these carriers were outsourcing the creation of lines of insurance, to provide coverage for specialized books of business for which they would likely have no prior experience underwriting, such as for cyber security.

documents, and other supporting documentation.[14] We were looking specifically for the coverage form, the application questionnaire, and the rate schedule, though not all forms were available for each policy.

Therefore, our analysis includes 180 individual filings from 2007 to 2017 from New York, Pennsylvania, and California. For each policy, we recorded the following metadata: the policy identifier (i.e. a unique identifier assigned by the state), state, submission date, the filing insurance company, the product name, the insurance line (discussed more below), and the insurance group.

We acquired policies from small and large carriers, for example, AIG, AXIS, Berkshire Hathaway, CUMIS, Chubb, Everest, Famers, Federal Insurance Company, Great American, The Hartford Steam Boiler Inspection and Insurance Company, Philadelphia, QBE, Travelers, XL, Zurich, etc. The product names (i.e. the names of the actual policies) include: Cyber Risk & Data Compromise Coverage, Cyber and Privacy Liability, Cyber & Security Incident, Cyber Cover Policy Program, Cyber One etc.

While some industry-specific policies (e.g. medical, financial) appeared, the vast majority of policies related to data breaches and privacy losses. The policies fell under the following property and casualty lines of insurance, as classified by NAIC:

- 01.0 Property/01.0001 Commercial Property (Fire and Allied Lines)
- 05.0 Commercial Multiple Peril (CMP) Liability and Non-Liability[15]
    - 05.0002 Business owners
    - 05.0003 Commercial Package
    - 05.0005 CMP E-Commerce
- 05.2 CMP Liability Portion Only / 05.2007 Other CMP
- 17.0 / 17.2 Other Liability-Occurrences/Claims Made[16]
    - 17.0000 / 17.2000 Other Liability Sub-TOI Combinations
    - 17.0001 / 17.2001 Commercial General Liability
    - 17.0019 / 17.2019 Professional Errors and Omissions Liability
    - 17.0022 / 17.2022 Other
    - 17.0024 / 17.2024 Internet Liability
- 26.0 Burglary and Theft/26.0001 Commercial Burglary and Theft
- 35.0002 Commercial Interline Filings

Notice that "cyber insurance" is not covered under a single line of business, but instead is distributed across multiple, related lines. Given that these policies were first adapted from professional errors and omissions (E&O) policies, these subcategories are not surprising (i.e. 17.0019 and 17.2019). Similarly, the other categories may be thought of as related forms of corporate liability policies.

We begin the analysis by examining the coverages and exclusions across policies, followed by a discussion of the security application questionnaires, and an analysis of the equations and methods used to derive the premiums. Note that policy identifiers have been anonymized using "POL-#," where the "#" symbol is replaced by a unique identifier.

[14] We omitted any policy that was filed but withdrawn.
[15] "The policy packages two or more insurance coverages protecting an enterprise from various property and liability risk exposures." -- http://www.serff.com/documents/PCPCM_0101-2015_updated0511.pdf.
[16] "Coverage protecting the insured against legal liability resulting from negligence, carelessness, or a failure to act resulting in property damage or personal injury to others." -- http://www.serff.com/documents/PCPCM_0101-2015_updated0511.pdf.

What do Cyber Insurance Policies Cover and Exclude?

Cyber insurance, like most insurance products, generally distinguishes between two broad loss categories, *first party* and *third party*. First party losses relate to those directly suffered by the insured (i.e. the "first" party to the insurance contract), while third party liability relates to claims brought by parties external to the contract (i.e. the "third" party) who suffer a loss allegedly due to the insured's conduct. As one might expect, most policies explicitly state that the insurer will pay the costs under the conditions that the cyber incident is a) discovered by the policy holder during the policy period, b) reported to the insurance company in a timely manner (usually 30 or 60 days from first discovery), and c) "provided that such costs are necessary and reasonable."[17]

Our analysis describes each of these categories in detail, based on examination of 54 policies in Pennsylvania, New York, California, and 15 policies captured directly from insurers' websites, filed between 2009 and 2016 (for a total of 69 policies). As we reviewed each new policy, we identified new criteria for coverage or exclusion, and developed a codebook to capture the main components of a policy. First we catalogued the types of policies available (i.e., types that fell under first or third party liability), for example "computer attack," "network security liability," and "personal data compromise." We then catalogued the losses covered by the insurance carriers for each type identified, adding new criteria for our codebook when appropriate. We also catalogued the exclusions enforced by the policies.

As we coded each policy we quickly found that the same controls were repeated – albeit not always in a standardized way. We identified 75 total controls: 17 relating to coverage, and 58 relating to exclusions.

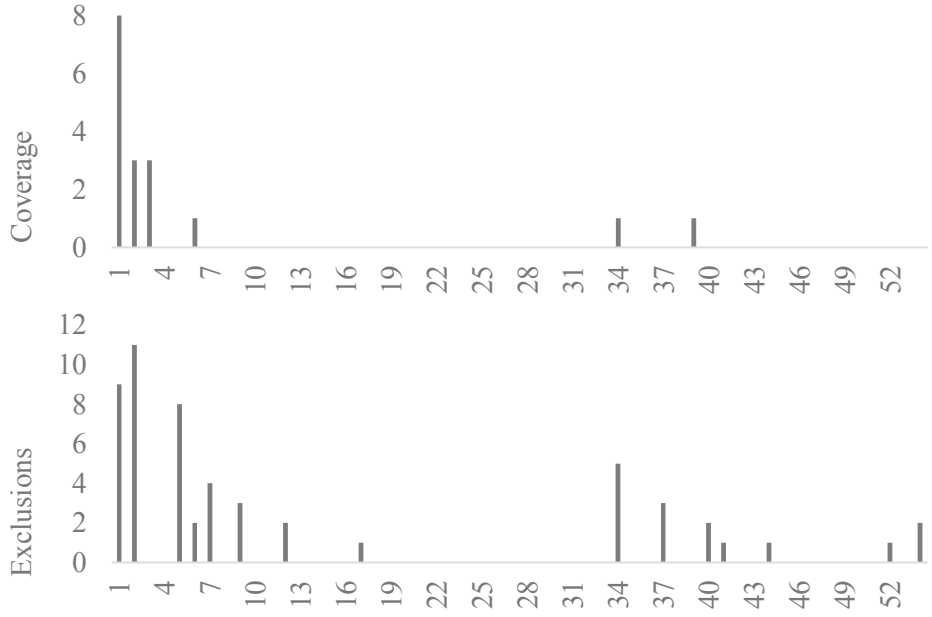

Figure 1 : Identification of Criteria over the Course of Reviewing Policies

As shown in Figure 1, we found that the controls for exclusions were more varied, while the controls for coverages appeared more standardized. That is, after reviewing 6 policies, we found that 88% of the criteria for *coverages* had been identified, while 52% of the criteria for *exclusions* had been identified.

[17] POL-24.

We find this consistency across policies to be surprising. From discussions with industry experts, the consensus is that there is so much variation within policies that examining a handful would provide no meaningful insights in to their coverage. The results presented above, however, suggest that there is, in fact, a strong overlap of both coverage and exclusions.[18]

First Party Coverage

As mentioned, first party coverage covers losses incurred directly by the insured. For example, it includes costs related to investigating the cause of a data breach or security incident, costs associated with restoring business services, the cost of notifying affected individuals, credit monitoring services, costs incurred from public relations and media services in order to communicate the event,[19] extortion and ransom payments,[20] and losses associated with business interruption.

In order to manage the various risks associated with these kinds of cyber incidents, carriers frequently assigned sub-limits (and in some cases, distinct premiums), to groups of first party losses. For example, some policies differentiated among just a couple of categories, such as personal data compromise and computer attack.[21] Personal data compromise relates to the "loss, theft, accidental release or accidental publication of personally identifying information (PII) or personally sensitive information."[22] A computer attack relates to unauthorized access, malware attack, or denial of service (DoS) attack on any computer or electronic hardware owned or leased and operated by the policy holder.

However, more sophisticated -- or perhaps, risk averse -- policies differentiated among more coverage areas, each with their own sub-limits. For example, POL-30 distinguished among the following groups as shown in Table 1.

Table 1: Four Coverage Sub-Limits

Coverage Area	Description
Data Compromise Response	"Provides coverage for specified expenses arising from a personal data compromise involving personally identifying information of affected individuals. Affected individuals may be customers, clients, members, directors or employees of the insured entity."

[18] In a number of cases, carriers would declare that firms from certain industries were ineligible to receive coverage. These industries included firms from adult business and gambling or gaming industries. In other cases, carries specifically excluded organizations involved in the sale or distribution of products regulated by the Bureau of Alcohol, Tobacco and Firearms, those involving use of pornographic data or images, or those with greater than 25% revenues generated from online sales. In one very restrictive case, the carrier considered firms within the following industries to be ineligible: education, healthcare, finance, government, publishing, data storage, website design, firms with websites containing information related to children, healthcare, entertainment/gambling, or sale of contraband or counterfeit items.

[19] See POL-126.

[20] See POL-127

[21] CyberOne policies commonly had these few number of differentiators. For example, POL-1covered both *personal data compromise* and *computer attack* for 1st party coverages, and *network security liability* 3rd party coverage, provided by CyberOne. Many other CyberOne policies (e.g., POL-17, POL-23, POL-47, POL-49) just included coverages for *computer attack* and *network security liability*, so it may be the case that separate coverage for *personal data compromise* is considered something additional.

[22] And, if PII is involved, it must result in or have the possibility in resulting in the fraudulent use of such information.

Identity Recovery	"Provides coverage for Identity Recovery caused by an identity theft of an identity recovery insured first discovered during the policy period."
Computer Attack	"Provides coverage for specified expenses arising from a computer attack on the computer system."
Cyber Extortion	"Provides coverage for the cost of an investigator retained in connection with the extortion threat and coverage for any amount paid by the insured in response to the threat."

Third Party Liability Coverage

As mentioned, third party liability covers the cost of defending against public or private litigation, settlements, judgments, or other rulings, as well as fines, fees, and settlements stemming from these lawsuits. For example, POL-35's network security liability coverage covers costs due to, "a civil action, an alternate dispute, a resolution proceeding or a written demand for money" as a result of "a [t]he breach of third party business information, [t]he unintended propagation or forwarding of malware, [t]he unintended abetting of a denial of service attack." [23]

Similarly with first party losses, coverage is available, and limits are distributed, across multiple kinds of claims. For example POL-30 distinguished between liability (brought by either a private or public action) due to a data compromise, network security incident, and electronic media as shown in Table 2.

Table 2: Three Liability Sub-limits

Liability	Description
Data Compromise	"[Provides] coverage for defense and settlement costs in the event that affected individuals or a government entity sue the insured because of a personal data compromise."
Network Security	"Provides coverage for defense and settlement costs in the event that a third party claimant sues the insured because of: • The breach of third party business information • The unintended propagation or forwarding of malware • The unintended abetting of a denial of service attack • The inability of an authorized third party user to access the insured's computer system."
Electronic Media	"Provides coverage for defense and settlement costs in the event that a third party claimant sues the insured alleging that the insured's electronic communications resulted in defamation, violation of a person's right of privacy, interference with a person's right of publicity or infringement of copyright or trademark."

[23] POL-111 covers first party losses stemming from crisis management expenses, security breach remediation and notification, computer restoration expenses, funds transfer fraud, extortion, and business interruption, as well as third party losses from network and information security liability, communication and media liability, and regulatory defense expenses. (POL-97) include coverage for, "Loss of Digital Assets, Non-Physical Business Interruption and Extra Expense, Cyber Extortion Threat, Security Event Costs, Network Security and Privacy Liability Coverage, Employee Privacy Liability Coverage Electronic Media Liability Coverage, Cyber Terrorism Coverage.

Variation Within Policies

Beyond the generalities defined above, below we describe a number of important variations observed from the analysis. Figure 2 shows the top 10 most common coverage topics for both state policies and large carriers.

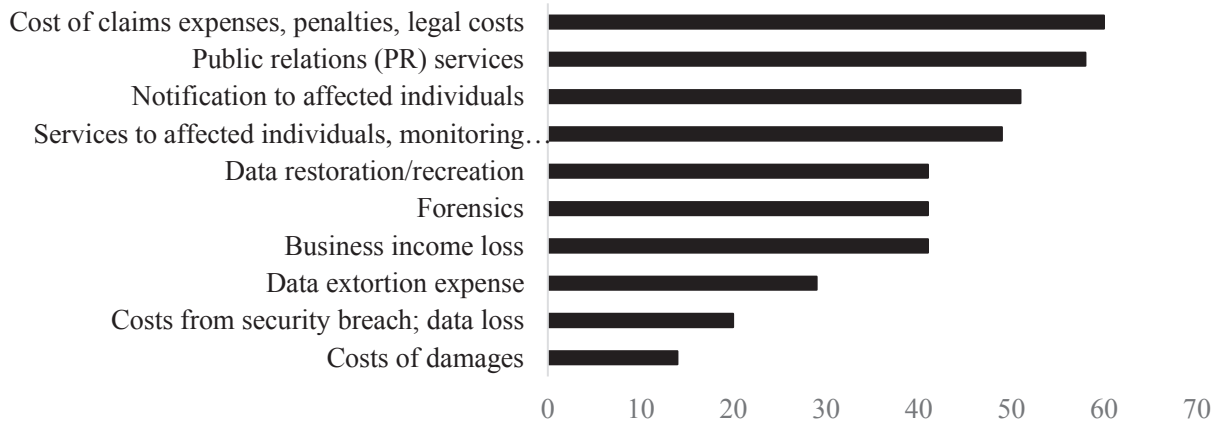

Figure 2: Total policies with observed coverages

Computer forensic costs

Expenses for computer forensic services (i.e. examining computer systems for indicators of malware or malicious activity) sometimes included the costs of computer expert services, and one policy (POL-22) noted that these expenses are specifically to be used in the case of disclosure of personally identifiable information (PII). For example, POL-22 states that, "If the incident involves an electronic security breach requiring computer expert forensic and investigation services … we will pay the costs of a computer security expert selected by you in consultation with our Breach Response Services Group from the program's list of approved security experts."

Notifications and additional services to affected individuals

Some policies are specific in terms of the kinds of services that can be provided to affected individuals – supplying a list of programs from which the policyholder must choose. For example, POL-22 requires that credit monitoring, identity monitoring, and fraud resolution services coverage only apply if Experian is used (specifically, Experian's ProtectMyID Alert, Family Secure, and DataPatrol.

Coverage for public relations (PR) costs appeared in the vast majority of policies, though sometimes came with restrictions.[24] For example, some policies only covered costs associated with advertising or special promotions, or in situations when a data privacy wrongful act had occurred.
Other policies limited the total dollar amount of coverage, or excluded any costs directed to employees, or when affected individuals had already been notified.

Claims expenses, penalties, defense, and settlement costs

Because claims expenses, penalties, defense, and settlement costs can be quite varied, policies that covered these costs often provided extra detail as to what was covered. For example, one policy (POL-20) defined that expenses would be paid for violation of timely disclosure of breach notice laws, regulatory and defense penalties, PCI Fines, claims against the reputation of anyone or any organization, the invasion of privacy, or any claims against website content to include copyright and plagiarism.

[24] As with the wide variation of types of coverage offered, specific elements like Public Relations services were listed under a variety of names: from the broad "computer attack coverage" to the specific "privacy breach expense coverages," "privacy notification costs," and "data compromise response expenses."

Items split between coverages and exclusions

About two-thirds of the policies covered expenses for data restoration, data re-creation, and system restoration, while most of the rest explicitly excluded costs incurred to examine or correct a deficiency (those with this exclusion provided (1) only the statement "cost to research or correct any deficiency" without any other explanation (POL-49); (2) a more, but still generic descriptions of the exclusion: the inspection, upgrading, maintenance, repair, or remediation of a computer system (POL-8; POL-19); or (3) more specificity of what it meant, for example exclusions of vulnerability review, physical security review, compliance with PCI or other standards, and damages to non-PII or non sensitive data (POL-1). Other expenses covered by many of the policies examined included business income loss (63%), data extortion expenses (41%), and forensic review (57%).

Aspects rarely covered

Only a few policies covered expenses resulting from acts of terrorism or war if perpetrated electronically (13%), costs of substitute systems used to resume activities (9%), and legal review (17%).

Exclusions

Figure 3 shows the 10 most common exclusions among the policies examined.

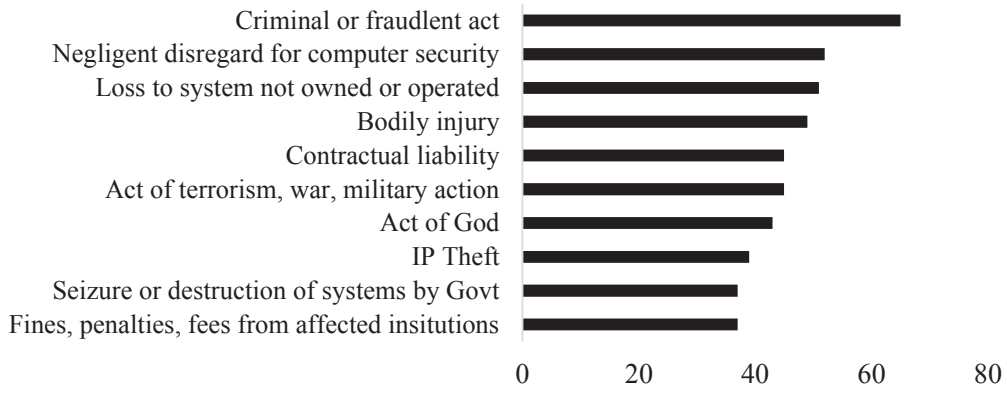

Figure 3: Total policies with observed exclusions

The exclusions most commonly observed were those not necessarily directly related to the cyber realm, but instead criminal, fraudulent, or dishonest acts, errors or omissions, intentional violation of a law, any ongoing criminal investigation or proceedings, and payment of fines, penalties, or fees. Several policies provide additional exclusions for infringement of patents, disclosures of trade secrets or confidential information, or violations of securities laws. We also found exceptions to the exclusions given certain circumstances (which themselves might have exclusions too). For example, in POL-22, any claims or losses arising from any deceptive or unfair trade practices are not covered – unless the claim results from the theft, loss, or unauthorized disclosure of PII, but only if no one involved in the deceptive or unfair trade practices participated or colluded in the theft, loss, or unauthorized disclosure.[25]

Other exclusions related to matters of physical harm (e.g., bodily injury, electric or mechanical failure, fire, smoke, wind or Act of God, release of pollutants), aspects of liability suits (e.g., non-monetary relief, and expenses resulting from the propagation or forwarding of malware on hardware or software created, produced, or modified by the policy holder for sale, damages related to employment discrimination,

[25] As can be seen by this description, parsing out the nuances in the policies can be a challenge: exclusions include exceptions that have their own exceptions buried in them.

contractual liability, theft of intellectual property), and losses to systems out of the policyholder's control (e.g., loss to the Internet, ISP, computer, or system not owned or operated by the policyholder). As mentioned previously, expenses for extortion or from an act of terrorism, war, or a military action were covered in rare cases, but mostly noted as exclusions.

Other rare but notable exclusions included:

- Collateral damage (i.e., malware, denial of service attack, or intrusion not directly aimed at the policyholder)
- Claims by any business in which insurance has a percentage of ownership (the percentage most commonly seen was 15%)
- Failure to disclose a loss of personally identifiable information (PII) if an executive of the firm was aware of such a loss
- Salaries, benefits, expenses of employees[26]
- Damages from outsourcing protected information or PII to non-US, non-Canada, non-EU[27]
- Claims on behalf of government organizations (to include federal, state, or local)
- Damages due to defects, deficiencies, or dangerous conditions of any of the insured products
- Unsolicited dissemination of communications

While there were no statistically significant differences in coverages found in state policies vs. those of large carriers, there were differences in exclusions. These differences are summarized in Table 3.

Table 3: Exclusions found more commonly/rarely in large carriers vs. state policies

Rarely seen in large carriers	More common in large carriers
• Cost to research/correct deficiency	• Property Damage
• Suit from propagation or forwarding of malware	• Seizure/destruction of systems/data by government
• Non-monetary relief	• Natural Elements
	• Unlawful collection or sale of information
	• Unsolicited Dissemination of Communication
	• Unfair Trade
	• Intellectual Property Theft

Summary

As consumers and firms adopt more technology and connected devices, there will likely be revisions to losses explicitly covered or excluded by cyber insurance policies. For example, one policy (POL-24) noted that expenses due to defects or deficiencies of the insured product were not covered. However, with the increase of the Internet of Things (IoT) devices, distributed denial of service (DDoS) attacks leveraging IoT devices, code reuse among products, and non-standardized software security practices of developers, exclusions may well become more frequent. We note that, while policies cited computers, networks, and systems, there was not explicit calling out of mobile devices or systems like drones and other IoT devices. It is unclear if these are grouped into the standard "computers, networks, and systems," or if carriers are even thinking about this new, but growing, group of devices.

Further, with the growing interdependencies of critical infrastructure across consumers, firms, and countries, exclusions for collateral damage or malware, denial of service attacks, or intrusions affecting government or private systems and networks will also likely increase. Perhaps carriers recognize the

[26] This exclusion was seen in four policies. Recall that one policy specifically included this as part of their coverage.
[27] One policy allowed for an exception to this exclusion if the protected information or PII was hosted in cloud-based storage.

increased likelihood of being a victim of collateral damage, and as such have decided to exclude coverages from claims resulting in this (over half of the policies we examined excluded any claims related to war, military action, or terrorist action; and almost half of the policies excluded claims related to extortion or ransom [although approximately a third *did* include coverage for extortion or ransom]). We might expect that more policies in the future will include similar exclusions, as the likelihood increases (along with the cost to recover).

How Do Carriers Assess an Applicant's Security Posture?

The next component of cyber insurance policies that we examine is the security questionnaires. These questionnaires are furnished by the carriers to the applicant and consist of a list of questions related to information technology, management, policy, and compliance practices adopted by the applicant. Ostensibly, these questions are used by the carrier to solicit a comprehensive understanding of (or at least reasonable approximation to) the overall security posture of the applicant, and to *differentiate* risks across applicants.

Note that under the broad category of cyber insurance, a wide variety of coverage includes media and liability for offered information, communication and technology (ICT) services or products. For instance, offline print media and broadcasting are sometimes covered in the same policies that offer cyber insurance. However, the analysis presented here focuses on cyber issues. Given that applications were not available for all policies, this section reflects the analysis from 44 questionnaires filed between 2009 and 2016 across California, Pennsylvania, and New York.[28]

In order to compare the questionnaires, they were each coded to identify commonalities in questions being asked. We identified 118 different topics, some of which were very detailed (e.g., "does the applicant deploy intrusion detection systems (IDS) or intrusion preventions systems (IPS)?") while others were quite broad (e.g., asking about general "business information"). However, many questions expressed similar themes, such as those pertaining to "business information," "data type," and questions regarding the compliance with PCI/DSS standards or the deployment of antivirus systems. Therefore, the 118 unique topics were classified into four main categories: Organizational, Technical, Policies and Procedures, and Legal and Compliance. Each is discussed in more detail in the following subsections.

We began the analysis with relatively rich and comprehensive questionnaires. The first questionnaire identified 48 unique elements; the second identified another 10; and 34 from the third. After reviewing just 3 questionnaires, 77% of all 119 information elements had been identified, and by 5 questionnaires, this number rose to 92% of all information elements. Figure 4 provides an overview of the new and prior informational elements found in each questionnaire. The number of questions in the applications ranged from 5 to 69, with a median of 26.5, and no questionnaire covered all 118 topics.

[28] Note that these 44 policies may not include the same subset of policies examined in the previous section.

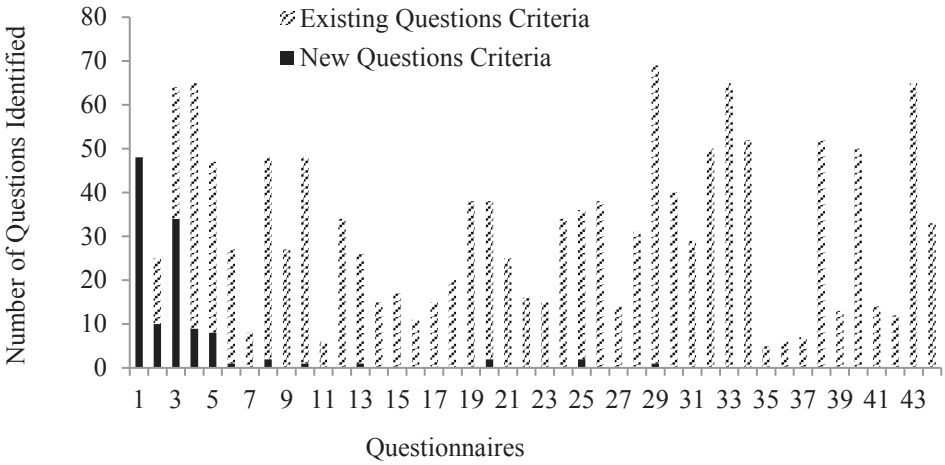

Figure 4 : Identification of Question Criteria

Organizational

General

The applications typically begin by collecting basic information about the company, such as the type of business and the industry sector in which the company operates, as well as financial information about revenues and assets. In a few cases, the questionnaires asked the company to submit an audited annual statement. For example, POL-7 asked for a "Copy of most recent financial statements (10-K, annual report, etc.)" in the questionnaire for its Professional, Technology, Media and System Security &Privacy Liability insurance.

To assess the operation of a business, POL-9 and POL-5 insurance policies gathered information about the insured clients, including who are the largest and/or most significant clients, the size of their contracts, and the duration of the project and relationship with the clients. POL-5 asks the insured to provide "details on the Applicant's top three (3) revenue-producing clients or projects during the last fiscal year," and POL-9 asks to "list the Applicant's five largest clients," including value and length of contract.

Information is also collected about the company's past and current insurance coverage, including selected deductibles, and exclusions, if applicable. This information, almost universally collected, likely helps the insurance company to evaluate the company's past dealing with carriers, and claims history.

Data Collection and Handling

Across the questionnaires, there was a concerted effort to understand the kinds of sensitive or confidential information that the application collects, stores, processes, or is otherwise responsible for. Of particular interest is personally identifiable information (PII), confidential client information, or corporate intellectual property. For example, questions related to the following data types: SSN, credit/debit card numbers, driver license, email addresses, IP addresses, financial and banking information, medical records, protected health information (PHI) as well as intellectual property, and trade secrets. For example, in its questionnaire for cyber liability insurance, POL-18 asked, "what Third Party electronic information the Applicant collects or stores: 'Medical/Health Information', 'Credit Card Information', and 'Personally Identifiable Customer Information, other than Credit Card or Medical /Health Information'."

In comparison with the "technology and infrastructure" category these questions focus on the kind of data an applicant is managing. This suggests that carriers focus on data and the potential loss at risk. This

possibly explains why relatively little information is collected about the technology and infrastructure landscape, or at least suggests that this category is less relevant when assessing an applicant's risk of filing a claim.

Outsourcing

Questionnaires also addressed how the applicant manages its relationships with outscoring providers and the services the applicant relies on to conduct business. Given that it is common to outsource services and/or use third party service providers, these questions were relatively common. Questionnaires asked the insured to list the outsourced services and provide the names of providers, and some even provided a comprehensive list for the applicant to select. For example, POL-22 asks whether, "the Applicant outsource[s] any part of the Applicant's network, computer system or information security functions."

Questionnaires further assessed whether a security, privacy, and/or risk assessment was performed on the third party provider. The history of the third party providers is assessed, with regard to whether they were subject to privacy or security breaches in the past. Further, contracts between the insured and the third party were examined, such as whether they were structured in a way to hold third parties liable for losses resulting from data and security breaches, or whether they included an indemnity clause to transfer risk to a third party. For instance, POL-18 asks "Does the Applicant's contract with the service provider(s) state that the provider: (a) Has primary responsibility for the security of the Applicant's information?; (b) Has a contractual responsibility for any losses or expenses associated with any failure to safeguard the Applicant's data?" In some instances, the questionnaire asked whether the insured requires the outsourcing provider to have sufficient cyber insurance to minimize any liability a customer can claim that results from an incident at the outsourcing provider (e.g., data or security breaches at the site of the outsourcing provider).

Incident Loss History

In almost all questionnaires, the insurer collected information about the insured experience with regard to past security incidents. While the formulation and framing of the questions varied across the questionnaires, in essence, the following issues were addressed: (a) past data and security breaches and their implications on the insured; (b) privacy breaches and loss of confidential information that triggered the notification of customers and/or employees; (c) circumstances that could lead to an insurance claim; (d) lawsuits and claims that are the result of an IP infringement; (d) extortions through the means of cyber, investigations by a regulatory or administrative agency. While other insurance companies often included multiple lengthy questions with regard to the security incident and loss history, POL-26 only one, "Has the Applicant had any computer or network security incidents during the past two (2) years? "[29]

IT Security Budget & Spending

IT security budget and spending provides insights into how much an insured invests in its information and IT security. However, IT security budgeting and spending was addressed in one questionnaire. POL-18 asked "What is the Applicant's aggregated budget for system security" and "How is the system security budget allocated among: (a) prevention of security incidents; (b) detection of security incidents; (c) response in security incidents, all in percentage."

[29] Where "incident" was defined as "any unauthorized access or exceeding authorized access to any computer, system, data base or data; intrusion or attack; the denial of use of any computer or system; intentional disruption, corruption or destruction of electronic data, programs or applications; or any other incidents similar to the foregoing? – Note: if the answer to Question III is "Yes", please attach a complete description of the incident(s), including whether the Applicant reported the incident(s) to law enforcement and/or the Applicant's insurance carrier."

Technical

Information Technology and Computing Infrastructure
Understanding the technology and infrastructure landscape of an insured would seem to be a relevant factor to consider in the risk assessment. Yet, only a few insurers cover this aspect in their questionnaire. When they did, only a few questions were posed, such as the number of computing devices, the number of IP addresses, or websites. For instance, POL-26 asked, "What is the Applicant's total number of IP addresses?" while POL-18 asks "List all website URL's and static IP addresses utilized by the applicant and its subsidiaries." In a few cases, policies asked whether the business' critical software was developed in-house. In another case, POL-52 inquired whether the insured segregated its IT systems that store and process PII from other parts of the network, "Are systems, applications and supporting infrastructure that collect, process, or store personal information segregated from the rest of the network?"

Information about the technology and infrastructure landscape would clearly help a carrier understand, if only at a basic level, the overall attack surface of a potential insured and, with more information, help assess their overall information security risk posture. However, it seems only very rudimentary information is collected.

Technical Security Measures
Technical measures to protect against data theft and intrusions were found in most questionnaires. These included questions concerning the kinds of tools used to secure the applicant's networks and computers, including anti-virus software to perform scans on email, downloads, and devices to detect malicious files or processes; IDS/IPS to detect possible intrusions and abnormalities in networks; and firewalls. POL-7 for instance, asks "Do you utilize firewall and intrusion prevention measures for your network and computer systems?" Encryption for data at rest and in motion was a technical measure that was often mentioned in the questionnaires. In its questionnaire, POL-7 asks, "Do you use commercial grade technology to encrypt all sensitive business and consumer information transmitted within your organization or to other public networks?" and "Do you use commercial grade technology to encrypt all sensitive business and consumer information at rest within your systems?" Some questions also focused on mobile devices. VPN and two-factor authentication were less frequently listed as technical measures.

From our analysis, questions regarding such technical measures were present in almost all applications. However, there was considerable variation in the types of questions that addressed technical measures. Further, as found questionnaires by POL-7 and POL-53, questions concerning re-application were shorter and often focus on key changes to address the business environment – as one might expect – rather than technical measures.

Access Control
Access control incorporates means and policies to secure user access, including the assignment of designated rights for users to resources. It attempts to restrict the access to sensitive data on a need to know basis. POL-54 asks, for instance, "Does the Applicant physically protect access to dedicated computer rooms and/or servers?" Beyond matters of access and users rights/privileges, questionnaires addressed whether processes were in place to revoke user rights and privileges once users terminated or left the organization. Furthermore, this includes the monitoring of unauthorized access to or large download of sensitive data, as well as remote shutdown and data wipe out capabilities for computers. Again, POL-54 asks "Does the Applicant utilize remote shutdown of employee laptops?"

Policies and Procedures

Information and Data Management
This category includes questions with regard to the applicant's data management practices – the number of records held, whether the applicant sells or shares sensitive information (i.e., PII) with third parties,

and whether it processes information for third parties, including the processing or storing of credit or debit card transactions. For example, one insurer in questionnaire POL-22 asks whether, "the Applicant process or store personally identifiable information or other confidential information (including but not limited to payment information) for third parties"

The most common question in this category was whether a data retention and destruction policy existed. For example, POL-54 asks "Does the Applicant maintain procedures regarding the destruction of data residing on systems or devices prior to their disposal, recycling, resale or refurbishing?" Interestingly, the questions do not exclusively address digital data, but rather, data management is conceived more broadly to also include written records that warrant protection (e.g., handling of sensitive information such as client or human resource information, etc).

The need for a corporate policy for record and information management and a classification system that determines what data must be protected was only expressed in a few questionnaires. In only one instance, did an application inquire whether the responsibility for records and information management was assigned to a senior executive.

Employee, Privacy and Network Security

Questions concerning an applicant's privacy policy, and information and network security policy were common but varied in detail. In some instances, the questionnaires assessed details of how a policy was implemented and tested, and whether a policy was reviewed by the legal counsel and approved by the board of directors. POL-9, for example, asks "Does the Applicant have Security and Privacy Policies that are updated continually and implemented and are there policies and procedures in place to ensure the Applicant is in compliant with requirements that govern the Applicant's industry?" If the applicant answers yes, the questionnaire continues to ask "If "Yes" have the policies been reviewed by a qualified attorney?"

While privacy, and information and network security policies were the most common policies mentioned in the surveyed questionnaires, usage policies for the internet, social networking, and/or email were mentioned. Less common were policies for software development (i.e., the use of secure coding standards), and password policies (e.g., the use of strong encryption).

However, aside from these, the questions did not cover the substance of a particular policy (i.e., what should be in those policies, and how should they regulate particular issues) but rather only tested their existence. In numerous cases, the questionnaires asked whether the responsibility of privacy and information and network security and their respective policies are assigned or "owned" by a Chief Privacy Officer (CPO) role and a Chief Information Security Officer (CISO) role, respectively. In most questionnaires, the CPO and/or CISO roles were explicitly stated, in rather few cases was it referred to as responsibilities assigned to an individual. For instance, in POL-9 asks "Does the Applicant have a designated person that is responsible for the management, implementation and compliance of the Applicant's security and privacy policies and procedures."

Organizational Security Policies and Procedures

In addition to technical measures that are implemented to protect the information system in the daily business operation, organizational measures and procedures describe a set of measures to maintain and strengthen information security. Questions in this category related to penetration testing, vulnerability scanning, assessment, and management. Further, questions related to security and privacy assessment conducted by internal first parties or external third parties were asked, as were measures with regard to physical security (e.g., physical access control to computing facilities). For instance, POL-18 asks "Does the Applicant run vulnerability scans or penetration tests against all parts of the Applicant's network? If "yes" how often are the tests run?" The applicant can then indicate the frequency by checking the box for

"Daily", "Weekly", "Monthly", or "Greater than Monthly." Several questionnaires assessed whether a business continuity plan (BCP), disaster recovery plan, as well as an incident response plan (IRP) were in place. Extended questions were concerned about the assignment of, and approval by, senior executives for the BCP and IRP. Further questions addressed data backup procedures as well as training with regard to information security procedures.

Legal and Compliance

Over the years, a variety of laws and regulations on the federal and state level, as well as industry standards have emerged that aim to protect consumers from the consequences of cyber incidents and data breaches. These laws, regulations, and standards are widely acknowledged in the questionnaires. Almost every questionnaire includes language about HIPPA, PCI/DSS, and GLBA, but also other U.S. federal and state laws. In some but not all cases, the questionnaires ask to provide metrics about how well the respective standards are implemented and adhered to. PCI as an industry standard for payment processing was prominent in many questionnaires. Further, questions concerning PCI/DSS commonly exhibit a significant amount of detail. For example, one insurer asks: "How many credit or debit card transactions does the Applicant process annually?" and then continues to collect information about whether the applicant: (a)Mask[s] all but the last four digits of a card number when displaying or printing cardholder data; (b) Ensure[s] that card-validation codes are not stored in any of the Applicant's databases, log files or anywhere else within the Applicant's network; (c) Encrypt[s] all account information on the Applicant's databases; (d) Encrypt[s] or use tokenization for all account information at the point of sale; or (e) Employ[s] point-to-point encryption, starting with card swipe hardware.[30]

Summary

So far, this analysis has provided insights into the information that carriers solicit of new applicants. For example, we observe an emphasis on assessing risk based on the amount of data (i.e., number of records) and the type of data (i.e., sensitive and confidential data) managed by the firm. The focus on sensitive data, particularly those to debit and credit card transactions and the detailed questions concerning PCI/DSS standard compliance, is not surprising given that in the past decade data protection industry standards and data breach laws have developed and have been widely institutionalized in the United States.

On the other hand, there is little attention given to the technical infrastructure, and its interdependencies with broader technological environment in which the applicant is operating. These rather technical areas could provide further insights into the risk situation and security posture of an applicant. With regard to organizational processes and practices, it was surprising that risk management and IT security management as corporate functions and processes did not receive more attention.

It's noteworthy, however, that standards and frameworks for information technology management, such as the ITIL and COBIT are not mentioned, and in only one instance was an ISO standard mentioned. Also, the recently developed NIST Cybersecurity framework is not mentioned, however, carriers are beginning to integrate this framework (and compliance therein) as a differentiating risk metric across applicants.

In addtion to the analysis described above, we did not observe any substantial changes in policy length, style, or composition over time. Conceivably carriers may develop institutional knowledge that would lead them to improve and refine the questions ove time, or, perhaps the questions would be found to be too generic, requiring more details solicited from applicants.

[30] POL-22.

Finally, only in one instance, did a questionnaire asked about the size of the IT/information security budget and how it is spent with regard to (1) prevention, (2) detection, and (3) response to security incidents. This finding was surprising given that amount of money spent on IT and information security could serve as a useful indicator for security maturity.

Next, we examine the process that carriers use for computing cyber insurance premiums.

How Do Carriers Price Cyber Insurance?

Cyber insurance underwriting has always been mysterious. How much do carriers know about cyber risks?; how do they assess these risks?; and, how are premiums actually computed? Not surprisingly, the answers to these questions are rarely, if ever, released or openly discussed. In this section, we examine the rate schedules from 96 distinct cyber insurance policies.[31] We first examine actual justifications used by carriers in determining how to price policies, and analyze the pricing schemes that carriers use to compute premiums. We conclude this section by showing the specific equations used to derive those premiums.

How much do carriers know about cyber risk?

In addition to the coverage and rate documents, the insurance forms that we acquired sometimes included justifications and explanations of the carrier's rates to the state insurance auditor. It is in these documents that we observe insights into the fascinating process by which insurance pricing is conducted, and what information carriers have in order to price cyber risk.

Overall, many carriers described how "cyber" is a relatively new insurance line, and that they have no historic or credible data upon which to make reliable inferences about loss expectations (e.g. "Limitations of available data have constrained the traditional actuarial methods used to support rates," POL-11). In these cases, firms either employed the services of other companies, such as the Hartford Steam Boiler Inspection and Insurance Company (HSB) or NAS Insurance in order to help develop premiums. Alternatively, or additionally, the carrier would collect industry, academic, or government reports to provide basic loss data. For example, many policies include explanations for such as:

> *"Frequency was derived from data gathered from the 2011 Computer Security Institute Computer Crime and Security Survey and from the HSB/Ponemon survey. Severities were calculated for three of the sub-coverages (data restoration, data re-creation and systems restoration) using data drawn from the HSB/Ponemon survey and from the 2003 Graziado Business Review which were then combined with dollar amounts that represented the costs of repairing various kinds of covered damages. These costs were obtained from a variety of IT repair resources, including surveys and published rates."*[32]

Or, in some cases, the carrier would appear to guess, (e.g. "The base retentions were set at what we believe to be an appropriate level for the relative size of each insured" (POL-6)), while many carriers

[31] "Rate schedules" or "rate development" are industry terms of art for the forms used to price premiums. Also, note that these schedules were not available for all policies acquired.

[32] POL-50. The same carrier also wrote, "HSB interviewed several lawyers that focus their practices in the cyber area and asked them to quantify, for each kind of dispute, how much it costs to take it to summary judgment, what percentage of disputes go beyond summary judgment, how much it costs to take the dispute to trial, etc. This expert elicitation process produced the severity estimates." While another carrier wrote, "According to a recent study commissioned by the Federal Trade Commission, 90% of all ID theft out of pocket expenses are $1,200 or less. We believe that the availability of case management restoration services will reduce this severity to approximately $230. The same FTC-commissioned report suggests a frequency of 3.66%. Thus, our loss content is expected to be $8.42. Loss-related expenses (toll-free help-line and case management service) are expected to be $3.00, resulting in a total IDR loss cost of $11.42. We added the loss costs together and applied our expense and profit load of 65.6% to arrive at our gross premium of $1,913.91." (POL-30).

employed what (limited) experience they had (e.g. “Rates for this coverage have been developed based upon the experience and judgment of our underwriters, claims personnel, and actuaries” (POL-25).

In some cases, carriers used external services, but then augmented them with additional information or their own, limited experience. For example one carrier wrote, “We reviewed the rates for a less robust cyber product developed by Hartford Steam Boiler (“HSB”) for the same types of accounts we are targeting[,] and then at a composite rate of the carriers writing more expansive cyber coverage for larger and more technologically sophisticated accounts. These two rates then became the two outside points of reference for establishing our rates” (POL-61).

Further, it was not unseen for carriers to examine their competitors in order to define rates, (e.g. “the rates for the above-mentioned coverages have been developed by analyzing the rates of the main competitors as well as by utilizing our own judgment” (POL-36), and “the program base rates and rating variables were based on a competitive review of the marketplace and underwriting judgment” (POL-31)).

In only a few cases were carriers confident in their own experience to develop pricing models, for example, one carrier wrote, “Underwriters collectively have over 40 years’ experience in e-commerce, cyber, privacy and network security liability insurance. The collective knowledge of underwriters, including a deep understanding of competitive rates and feedback from the wholesale and retail brokerage industry, was used to establish rates for the program” (POL-2).

In a number of instances, we observed how carriers would turn to other insurance lines to price premiums because of their lack of data. One carrier admitted, “We are not using claim counts as the basis for credibility because we have not experienced any claims over the past three years” (POL-73). And in such cases carriers would base cyber risks on other insurance lines. For example, “Loss trend was determined by examining 10 years of countrywide Fiduciary frequency and severity trends. Because CyberRisk is a developing coverage we chose to use Fiduciary liability data because it has a similar limit profile and expected development pattern.” (POL-43). Other carriers also leveraged loss history from other insurance lines, “the Limit of Liability factors are taken from our Miscellaneous Professional Liability product,” (POL-25), and “Base rates for each module of this new product were developed based on currently filed Errors and Omissions and Internet Liability rates” (POL-104).

In conclusion, regardless of the formal (and sometimes very informal) methods used in the underwriting process, it appears that state regulations require that carriers be vigilant about ensuring fair and accurate pricing. This is done, in part, by ensuring the underwriters are empowered to adjust premiums appropriately, when necessary, (e.g.“The rating modifiers…allow the underwriter to debit or credit the policy premium based on the unique attributes of an insured. These modifiers reflect objective criteria associated with the cyber risks and controls of an insured” (POL-6)). And further, this required concrete advisors by insurance auditors, where one auditor wrote, “Please be advised that the company is required to maintain statistical data, including incurred losses and loss adjustment expenses, on reported and unreported and outstanding and paid categories, on this program separate and apart from its other coverages. In addition, the experience should be reviewed annually, and appropriate rate revisions filed, (POL-49)” to which a number of carriers replied, “[w]e will monitor our book’s performance as we develop our own experience to ensure that our product remains competitive and profitable” (POL-63).

Next we examine the actual rate schedules and analyze the methods used to price cyber insurance premiums.

How do carriers assess cyber risk?

Unlike the analysis presented above for the coverage and questionnaire sections, we found that the calculation of premiums across carriers exhibited much less variation in structure and composition.[33] Indeed, some policies offered simply a flat rate to all applicants, while other policies adjusted that price according to select variables.

Of the non-flat rate pricing, there were three broad categories of variables used: those relating to the applicant's assets/revenue, those relating to standard insurance criteria (e.g. limits, retention, claims history, etc.), those relating to the applicant's industry, and those relating to the applicant's information security posture. Because the first three categories are standard to all lines of insurance, and the last category (information security controls) is of primary focus for this research, we therefore classify the rate schedules into three categories: *flat rate pricing*, *base rate with modifications*, and *information security pricing*. Table 4 provides descriptive statistics on the number of variables used, by policy type, in the computation of a premium

Table 4 : Number of Variables Used to Compute Premium

Policy Type	Min	Max	Mean	N (Policies)
Flat Rate	-	-	-	31
Base Rate	2	21	11.7	31
Security	1	20	7.0	34
				96

We next examine each of these policy types in detail.

Flat Rate Pricing

The simplest approach to computing premiums used by 31 (32%) of the 96 policies defined a single rate for each first and third party coverage to all insureds. While this approach offers a quick method for establishing premiums, it affords no differentiation by firm or industry. For example the CyberOne policy, developed by Insurance Services Organization (ISO), is used by many smaller insurance companies and offers first and third party premiums as shown in Table 5.

Table 5: Simple Rate Development

Coverage	Frequency	Severity	Expected Loss (Lost Cost)	Profit Load	Premium
Computer Attack	0.20%	$49,800	$99.60	35%	$153
Network Security Liability	0.17%	$86,100	$147.23	35%	$227

The frequency column represents the probability of a given loss event, computed annually, while the severity reflects (presumably) the mean annual loss. The expected loss column is simply the product of the first two columns, and the profit load is the standard method by which insurance carriers cover costs and expenses. Note that while this approach was used by many carriers, there was some variation across carriers with regard to the frequency, severity, profit loading, and therefore premiums as they incorporated other information.

[33] Though, actual pricing did vary, of course.

For context, in other research that examined the cost of cyber incidents, the median cost was found to be $170,000, with a probability of loss around 0.6% across the top 10 most risky industries, producing an expected loss of $1020 – considerably higher than the values shown above (Romanosky, 2016).

The final premium is then a function of the expected cost, and the profit load of 35%. From the policies examined in this research, profit loading ranged from 25% to 35%. Factoring in the profit loading then produces the final premiums of $153 and $227 for computer attack coverage and network security liability coverage, respectively.[34] Note that these premiums typically apply to policies with limits of $100,000 and deductible of $10,000.

Overall, this approach is simple and straightforward. However, it relies entirely on estimates of frequency and severity of cyber events and litigation costs. We examine the source of these numbers in the next section.

Next, we discuss the second, more sophisticated approach using base rate pricing.

Base Rate with Modifications

31 (32%) of the policies in our analysis used base rate pricing.[35] That is, a base premium is assessed as a function of the insured's annual revenues or assets (or, with some niche products, number of employees or students). This base premium is then adjusted according to (multiplied by) multiple variables relating to standard insurance and industry-related factors. We describe the base rate approach first, followed by the standard insurance properties, and then the industry-related factors.

The factor that assigns the greatest influence on the premium is the base asset value or revenues of the applicant's firm. For example, Table 6 provides one example of how a policy initially defines the premiums, as a function of firm revenue.

Table 6 : Base Premiums By Revenue

Revenue (in millions)	Annual Gross Base Premiums
$0 - $10	$1,913.91
$10 - $20	$2,602.92
$20 - $50	$3,502.46
$50 - $100	$5,224.98

And Table 7 shows premiums with associated retention (deductible) by asset size.[36]

Table 7: Retention by Asset Size

Asset Size (in millions)	Base Rate	Base Retention
to $100	$5,000	$25,000
$100 to $250	$7,000	$25,000
$250 to $500	$8,500	$50,000
$500 to $1,000	$11,000	$100,000

[34] i.e. $99.60 / (1 - 0.35) = $153

[35] Not to be confused with a statistical base rate or the base rate fallacy.

[36] POL-6.

$1000 to $2,500	$14,000	$150,000
$2,500 to $5,000	$16,500	$250,000
$5,000 to $10,000	$20,000	$250,000
$10,000 to $25,000	$26,000	$500,000
$25,000 to $50,000	$35,000	$500,000
$50,000 to $75,000	$41,000	$1,000,000
$75,000 to $100,000	$45,000	$1,000,000

Table 8 provides a sense of the variation in premiums found in our analysis across carriers, for a firm with $100 million in sales (or assets), a $1 million limit and $10,000 deductible. Notice the range from just $3,300 to over $7,500 (with one policy charging a drastically higher premium, but with $0 retention/deductible). These prices, of course, would not reflect the final price, but it does present one perspective in pricing.

Table 8 : Variation in Premiums for $100m in sales or assets

Policy	Premium
POL-55	$3,300
POL-41	$3,500
POL-56	$3,965
POL-37	$4,000
POL-6	$5,000
POL-88	$6,000
POL-32	$7,500
POL-33	$42,000[37]

Standard Insurance Factors

Standard insurance factors include variables such as changes to the limits or deductible (retention) of a policy. For example, the greater the limits, or the smaller the deductible, the larger will be the premium, as shown in Table 9.

Table 9 : Limits Factor

Limits	Factor
$500,000	0.809
$1,000,000	1.000
$2,000,000	1.132
$3,000,000	1.245
$4,000,000	1.371
$5,000,000	1.405

In addition, the premium will be modified based on factors such as coinsurance, time retention, prior acts, extended reporting period, and business interruption. Co-insurance adjusts for whether the insured carries coverage with other carriers. Time retention and extended reporting period adjust for the length of time an insured signs the contract, and is decreasing the longer is the insurance contract.

[37] For a $0 retention.

Historical claims refers to the number of times the insured has suffered an incident and filed a claim in past years. Premiums typically increase about 10% for each event.[38] However, one carrier provides a more descriptive offering for claims history, as shown in Table 10.[39]

Table 10: Claims History

Category	Min	Max
Very Favorable	0.75	0.85
Favorable	0.9	0.99
Average	1.0	1.0
Slightly Unfavorable	1.01	1.15
Materially Unfavorable	1.16	1.25
Very Unfavorable	1.26	1.4
Extremely Unfavorable	1.41	1.7

A few policies provided coverage for business interruption in the event of a data breach or security incident. For example, POL-2 defined the additional cost of business interruption as shown in Table 11.[40]

Table 11 : Business Interruption

Industry	Waiting Period	Business Interruption Charge
Auto Dealership	10 hrs	10.0%
Automotive Services	10 hrs	10.0%
Domestic Services (e.g. plumbers, electricians, gardeners)	8 hrs	5.0%
E-commerce	24 hrs	50.0%
Education - Colleges / Universities / Higher Education	8 hrs	5.0%
Professional Services (excluding Legal Services)	12 hrs	25.0%
Realtor - Commercial / Residential	10 hrs	10.0%
Restaurant	10 hrs	10.0%
Retail	24 hrs	50.0%
Sports Clubs / Gyms	8 hrs	5.0%
Telecommunications	24 hrs	50.0%

Industry Classification

Next, carriers attempt to control for risks to the insured based on the industry in which it operates. However, from the policies examined in this research, there was no consistency regarding approach, or any consensus on what the insurance industry would consider the "most" risky.

POL-18 assigns the energy, entertainment and hospitality sectors a weighting of 1.0 (meaning no adjustment – essentially neutral risk), while firms in the accounting, advertising, construction, manufacturing industries receive a weighting of 0.85 (less risky), and firms in the bio-tech, data aggregation, gaming, and public sectors receive a weighting of 1.2 (more risky). How these relative weightings are determined is unclear and never described.

Some policies are very simple in their approach and define only 3 hazard groups:[41]

[38] POL-32.
[39] POL-33.
[40] For brevity, we only show a sample of the full table.
[41] POL-38. See also POL-40 and POL-44.

- Low Hazard Classes possess a low amount of Personally Identifiable Information. Examples of these classes include most farming and agriculture risks.
- Medium Hazard Classes possess low to moderate value and volume of Personally Identifiable Information. Examples include Wholesale Operations and warehousing.
- High Hazard Classes possess moderate to high value and volume of Personally Identifiable Information. Examples include Retail and Merchant store operations.

Another carrier distinguished among 4 hazard classes with premium modifiers as shown in Table 12.[42]

Table 12 : 4 Hazard Classes

Class	Description	Factor
1	Businesses whose primary personal information is relative to employees	0.804
2	Businesses that keep financial or account number information on individual customers but do not keep customers' Social Security numbers	1.000
3	Businesses with customers' Social Security numbers	1.497
4	Entities that collect and store a high volume of particularly sensitive personal information, are at high risk of loss or theft of that information and are subject to structural restraints on their security spending	1.905

Notice how Class 2 (firms which process financial information) is assigned the datum, implicitly stating that SSN and high volume transaction information are considered more risky. Further, notice that 4 significant digits are used for these factor weightings. It is unclear how these figures were derived, or whether such precision at all accurately reflects true risk.

Another carrier takes a more aggregate approach by differentiating non-profit, for-profit, and only a few other industries, as shown in Table 13.[43]

Table 13: Industry Risk

Industry Classification Factor	Weighting
Non-profit, Non-medical	1.0
For Profit, Manufacturer	1.5
For Profit, Wholesale	1.5
For Profit, Non-technical service provider	1.5
Computer Consultants	2.0
System Integration	2.0
Software Manufacturer	2.0
Retail	3.0
Healthcare	3.0
Accountants	3.0
Financial	4.0
Large Risk (over $250M revenue)	5.0

[42] POL-30.
[43] POL-32.

All other	3.0

Next we examine the factors seen in the most sophisticated and detailed policies – those that account for information security controls by the applicant.

Information Security Pricing

The most sophisticated approach used by the policies examined in this research accounted for characteristics of the applicant's information security controls when determining the final premium pricing. 34 of the 96 (35%) incorporated some form of information security considerations into the premium calculation.

Adjustments based on the applicant's actual security posture vary widely across polices, ranging from basic risk categories to more detailed metrics. One very simple approach considers broad categories of data protection, and adjusts based on qualitative ratings above or below what one may consider to be "average" maturity of controls, as shown in Table 14.[44]

Table 14 : Basic Security Modifiers

Category	**Modification**		
	Below Avg	Avg	Above Avg
Privacy Controls	1.20	1.00	0.80
Network Security Controls	1.20	1.00	0.80
Content Liability Controls	1.20	1.00	0.80
Laptop and Mobile Device Security Policy	1.10	1.00	0.90
Incident Response Plan	1.10	1.00	0.90

While simple (and possibly appropriate), this particular policy provides no guidance on how an underwriter is supposed to assess an applicant based on these properties. For example, there is no rubric provided as to differentiate "Below Average" from "Above Average" or even what would be included in a firm's collection of privacy controls.

A slightly more detailed and thoughtful approach was found in POL-64 which differentiates a firm's overall security posture along 6 dimensions (factors): data classification, security infrastructure, governance, risk and compliance, payment card control, media controls, and computer system interruption loss. Each factor provided 4 qualitative options (poor, fair, good, excellent) with a weighting as shown in Table 15.

Table 15 : Security Factor Weighting[45]

Rating	**Weighting**
Excellent	0.75-0.85
Good	0.85-1.00
Fair	1.00-1.25
Poor	1.25-1.50

The benefit of this approach relative to other simpler or more complex approaches is that it affords a reasonable tradeoff between specificity and practicality. For example, other polices adjust the premium

[44] POL-44.

[45] Source POL-64. See also POL-41.

based on specific answers to self-assessment questionnaires (whether the firm uses 2-factor authentication, industry standard firewalls, proper best practices), it is highly unlikely that any insurance underwriter would know the marginal reduction in risk that any of these provide. The information simply doesn't exist to determine a meaningful answer. Therefore, this approach affords the underwriter the ability to investigate a firm's controls and make reasonable assessments. This policy also intelligently provides useful scoring rubrics for each category. For example, the data classification category describes the following:

> *"The Data Classification Factors are determined by assigning a hazard group factor which is based on the type(s) of data handled, processed, stored or for which the Insured is otherwise responsible for safeguarding. Examples of Data Types are credit card numbers, financial account information and/or personal health information. The appropriate factor should be applied multiplicatively. What type of data is processed, stored or maintained by or on behalf of the insured? Can the data be used to create a false identity, i.e., SSN, DOB, or not, i.e., e-mail address, passwords? Is the data subject to regulation (federal or state), i.e., protected health information (PHI) under HIPAA or driver's license numbers (PII) under state notification laws, etc. Does the data include corporate confidential information of a third party, such as trade secrets and intellectual property?"*

Other policies took another approach to adjust the premium based on the firm's responses to each question from the application (i.e. security questionnaire). For example, POL-6 included the following adjustments such as shown below.

(3) Is the disaster recovery plan tested at least annually? Answer YES to	Factor
Three of the above questions	0.80 to 0.90
Two of the above questions	0.91 to 0.99
One of the above questions	1.00 to 1.05
None of the above questions	1.06 to 1.15

(4) Did the total number of targeted computer attacks increase, decrease or remain unchanged in the past 2 years?	Factor
Decrease	0.85 to 0.95
Unchanged	1.00
Increase	1.10 to 1.20

(5) Are penetration tests conducted on the insured's network at least annually?	Factor
Yes	0.85 to 0.95
No	1.10 to 1.20

How are premiums finally computed?

From the policies examined (except for the flat rate pricing policies), once the base asset/revenue value is determined, the final premium is computed as the linear product of each of the factors contained in the rate schedule. One policy describes the process as, "*Pricing is calculated by applying modification factors*

to a base premium. The modification factors are determined by various criteria including the Limit of Liability and Deductible purchased, the coverage enhancements or restrictions negotiated with the insured, and the risk's financial characteristics. All modification factors are multiplicative, unless otherwise indicated."[46]

As described, for some policies, there may only be a few factors, while for others there may be many. For example, the premium in one policy is computed as:[47]

Premium = [Base Premium] x
[Loss Rating] x
[Professional Experience] x
[Longevity of Operations] x
[Use of Written Contracts] x
[Risk Characteristics] x
[Prior Acts Factor] x
[Coverage Adjustment] x
[Deductible],

While another formula is composed of 6 groups of factors and 13 separate security-related questions, producing a final expression of:[48]

Premium = (Section 1 Base Rate) x
(Section 2 Industry Factor) x
(Section 3.1 Increased Limits Factor) x
(Section 3.2 Retention Factor) x
(Section 3.3 Coinsurance Factor) x
(Section 6 Third-Party Modifier Factors)

Another policy further extends expands the security properties, producing the following expression:

Final Premium = (Third Party Liability Base Rate) +
(First Party Costs Base Rate, if elected) x
(Limit Factor) x
(Retention Factor) x
(Data Classification Factor) x
(Security Infrastructure Factor) x
(Governance, Risk and Compliance Factor) x
(Payment Card Controls Factor) x
(Media Controls Factor) x
(Computer System Interruption Loss Factor, if applicable) x
(Retroactive Coverage Factor) x
(Claims/Loss History Factor) x
(Endorsements Factor, if applicable)

Summary

From our analysis, the first and most important firm characteristic used to compute insurance premiums was the firm's asset value (or revenue) base rate, rather than specific technology or governance controls. This appears to be the single most common proxy for firm size, and therefore risk.

[46] POL-20.
[47] *Id.*
[48] POL-6.

While some carriers have sophisticated algorithms for premium estimates, policies that cater to small business are very simple. In addition, premiums that capture third party losses (i.e. liability coverage) are generally more costly than those associated with first party losses, suggesting that carriers expect legal actions to be more expensive relative to direct losses suffered by the insured.

While a few carriers incorporate specific information collected from the policy's security self-assessment forms, many policies used more generic security risk categories (e.g. high, med, low). And while many policies incorporate industry factors into the underwriting process, no explanation or justification for how the actual risk weighting is provided. Further, the industries listed rarely match standard coding schemes like SIC or NAICS.

Beyond the specific equations, however, it is unclear which level of sophistication of premium calculation is optimal for the firm, and is best able to assess an applicant's risk. Indeed, this remains an outstanding issue among carriers.

Cyber Insurance Litigation

The volume of cyber attacks in recent years has highlighted material gaps in coverage for both commercial general liability (CGL) policies and standalone cyber policies. As this market is relatively young, language regarding coverage is still evolving, and there are many potential exclusions which the insured may overlook when selecting a policy. While lawyers often counsel insured to buy standalone cyber coverage on top of CGL (Rand, 2017), even the combination of the two may not be enough to protect the insured from costly losses in the event of a cyber attack.

First, is the matter of first vs. third party coverage. As mentioned, first party coverage generally includes forensic investigations, breach notification costs, and costs related to data loss/damage, while third party coverage covers lawsuits and regulatory fines and investigations. *Camp's Grocery, Inc. v. State Farm* (10/25/2016) was a prime example of the need to pay attention to first vs. third party liability coverage in insurance policies. Camp's was sued by several credit unions after a data breach, and it was ruled that Camp's CGL policy excluded third party coverage. The ruling explicitly noted that insurance policies typically cover either first or third parties, suggesting that policies that cover both are necessary (as provided in many standalone cyber policies; Rand 2016a).

Additionally, the cause of the compromise is also vital in determining liability. *Zurich American Insurance Co. v. Sony Corp. of America* (2/21/2014), found that Sony's CGL policy did not cover the theft of personal identifiable information (PII) by the hackers, as it was not the policyholder that caused the information release, but rather a third party (Armenti and Cantarutti, 2016).

"Publication" of information is also not usually defined in CGL policies; dissemination could be to the broad public or one individual, and there is also a question of whether publication implies only the potential accessibility of information, or its actual use. *Recall Total Information Management, Inc. v. Federal Insurance Co.* (5/26/2015) found that no coverage was warranted when IBM lost a number of tapes containing PII, but could not prove the tapes were accessed. In contrast, *Travelers Indemnity Co. of America v. Portal Healthcare Solutions* (4/11/2016) found that publication of PII on the internet was a public release of information that should be covered by the insured regardless of proof of access (Armenti and Cantarutti, 2016). While many hoped that the *Travelers* ruling would imply more liberal coverage of PII publication in the future, Dilworth Paxon LLP argues that CGL policies since the writing of *Travelers* (in 2012/2013) have explicitly excluded coverage for lawsuits arising from data breaches (ISO standard exclusion CG 21 06 05 14), and thus it is unlikely that similar cases in the future will be decided in favor of the insured (Rand 2016b).

Other explicit exclusions are commonly found in CGL policies under Coverage A and B. In Coverage B, a number of exclusions to CGL may prevent coverage of damages readily available under another policy. In *National Union Fire Insurance Co. of Pittsburgh, Pa. v. Coinstar, Inc.* (2/5/2014), the insured was found to violate a state statute regarding transmission of information, an exclusion explicitly listed in the policy, and thus was not covered. However, in *Hartford Casualty Insurance Co. v. Corcino & Associates* (C.D. Cal. 10/7/2013) found that despite the Coverage B exclusion due to statute violation, the insurer was responsible for liability for damages that would have occurred absent the existence of such an act. The treatment of Coverage B exclusions and alleged statutory violations is not uniform, suggesting that future court rulings may set precedent in this area (Armenti and Cantarutti, 2016).

Yet another murky realm with regard to coverage of CGL policies is whether or not the loss of data counts as property damage. In *Carolina Casualty Insurance Co. v. Red Coats, Inc.* (4/22/2014) the district court ruled that the theft of laptops with PII did not constitute property damage, as the policy excluded electronic data from the definition of property damage, and the PII was not rendered unusable/lost. Upon appeal, this decision was vacated due to a failure of the district court to determine whether exclusion of electronic data was dependent on state law; no further decision was reached due to settlement by the two parties in question. *Nationwide Insurance Co. v. Hentz* (3/6/2012) found that the theft of a CD-ROM from an insured accountant was covered by her homeowner's policy, as the CD-ROM was tangible property; it did not enumerate whether the ruling would apply to solely electronic data (Armenti and Cantarutti, 2016).

Even for actual physical damage incurred (e.g., control taken over an automated system that results in a physical accident), it is not clear that this damage is covered under most CGL policies, as many exclude damage "arising out of" cyber attacks. There has not yet been definitive litigation on the subject (Rand 2016c). Standalone cyber policies usually also exclude physical damage, implying that additional gap coverage is needed for a comprehensive plan (Rand 2017).

In addition to the gap created by physical damage, social engineering is another topic that is not necessarily covered by typical CGL or standalone cyber policies. *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh, PA* found that the insured was not covered due to an authorized user's input of information to transfer funds to a fraudulent source, rather than unauthorized entry. In contrast, the opposite was found in *Apache Corporation v. Great American Insurance Co*., in which the use of a computer to fraudulently transfer funds (as covered in the policy) was deemed to include an authorized user emailing the information to the social engineer (Rand 2016d). Coverage also exists to fill this social engineering gap, which the FBI has estimated has cost at least two billion in losses since 2015 (Rand 2017).

While most cases thus far have involved policies with cyber endorsements, one of the first standalone cyber insurance lawsuits was *Travelers Property Casualty Co. of America v. Federal Recovery Services, Inc.*, in which Federal Recovery withheld data from Global Fitness due to a payment dispute. The court ruled that Federal Recovery was not insured by technology errors and omissions liability, as it willingly withheld data from Global Fitness. Such a dispute regarding the coverage of intentional and non-negligent acts under errors and omissions policies is common under traditional insurance realms; in most instances courts have found that intentional and non-negligent acts are still covered. As K&L Gates LLP points out, this ruling has several important lessons for the general cyber insurance market—" Until the governing law applicable to an insurance contract—"cyber" or otherwise—is established, the policy can be, in a figurative and yet a very real sense, a blank piece of paper", and it is vital to focus on language at initial coverage/renewal stages, as cyber policies are much more negotiable than traditional policies (Anderson, 2017)

One additional recent case, *P.F. Chang's China Bistro Inc. v. Federal Insurance Co.*, determined that P.F. Chang's was contractually obligated to pay Bank of America Merchant Services as a third party for the loss caused by its data breach, as P.F. Chang's policy explicitly excluded contractually assumed liability, an exclusion common in CGL policies. This exclusion, as Dilworth Paxon LLP points out, is one that could easily be struck from an insurance contract with negotiation.

Summary

Due to the growing nature of the cyber insurance industry, and the consequent lack of standardization of policies, some of the uncertainties are being resolved in the court room rather than between insurers and the insured. Most cyber insurance lawsuits thus far have questioned the coverage of cyber endorsements of previous policies rather than standalone cyber insurance, suggesting that endorsements may obfuscate critical areas such as the differences between first and third party coverage. Another hotly contested area is an insurer's responsibility to cover physical damage either under commercial general liability (CGL) policies or standalone cyber polices; this is often written into a policy's exclusions, and some policies may go as far to exclude events such as pollution created by a cyber attack. Social Engineering is yet another realm that is often not covered by either CGL or standalone cyber policies, but may be purchased as separate gap coverage. Much of this litigation could be avoided through the careful writing of cyber policies, given that the nature of the industry also makes insurers much more flexible about amending coverages/exclusions.

Limitations

There are a number of important limitations to this research. First, our analysis and conclusions reflect results based a sample of all insurance policies covered in the US. Naturally, this suggests that further analysis incorporating more policies across more states may reveal additional or even different results. However, that being said, based on our previous examination of state regulations pertaining to the insurance industry, we have no *a priori* reason to believe that there will be any material differences across US states, or that our findings would change in any material way.

The second potential limitation concerns the matter of admitted versus non-admitted markets. If it were true that most cyber insurance coverage were written in the non-admitted markets (i.e. markets that we do not observe), this would reduce the generalizability of our results beyond just the non-admitted market. In effect, we would only be observing a sample of the overall population of polices. However, based on our preliminary analysis of the coverages and applications, we see no material differences in policies between these markets. That being said, we are unlikely to observe the rate schedules and algorithms for many policies within the non-admitted market.

Conclusion

This research has presented the first analysis of actual cyber insurance policies. We collected 180 policies from New York, Pennsylvania, and California, as well as policies posted publicly on carriers' websites, and separately examined three main components: the coverage, the application questionnaires, and the rate schedules.

Overall, we find that there is a very strong similarity across the coverage topics of these policies, with a much greater variation in the exclusions imposed. For example, after examining only 6 policies, 88% of the coverage topics had been identified, while only 52% of all exclusions were documented.

The questionnaires, as part of the required regulatory filings by insurance firms in the admitted market, give interesting insights about what information is (and is not) collected. However, they do not provide insights about whether and if what additional information insurers may acquire from third-party providers

to assess risk beyond the level of a single insured entity (e.g., industry and market risk regarding cybersecurity). For instance, risk information about the security posture of third-party service (e..g. cloud) providers and intermediaries that an insured relies on, may be difficult to obtain from a single insured entity. Yet, an insurer may have interest in the risk posture of a service provider that accumulates risk across multiple insured entities. A cloud computing provider may be such an example due to the dependencies of multiple insured entities covered by a single insurer. Such risk information may be elicited from other sources than a security questionnaire.

Finally, regarding the rate schedules, we found a surprising variation in the sophistication of the equations and metrics used to price premiums. Many policies examined used a very simple, flat rate pricing (based a single calculation of expected loss), while others incorporated more parameters such as the firm's asset value (or firm revenue), or standard insurance metrics (e.g. limits, retention, coinsurance), and industry type. More sophisticated policies included information regarding information security controls and practices as collected from the security questionnaires.

By examining these components of insurance contracts, we hoped to provide the first-ever insights into how insurance carriers understand and price cyber risks.

References

Airmic. (2012). *Airmic Review of Recent Developments in the Cyber Insurance Market*.

Allied Market Research. (2016). *Cyber Insurance Market — Global Opportunity Analysis and Industry Forecasts, 2014-2022*. Retrieved from http://www.businessinsurance.com/article/20161207/NEWS06/912310865/Cyber-insurance-market-to-grow-says-Allied-Market-Research

Anderson, Roberta D. (21 May 2015). Five Takeaways from the First Cyber Insurance Case. K&L Gates, LLP. Retrieved from http://www.klgates.com/five-takeaways-from-the-first-cyber-insurance-case-05-21-2015/. Last accessed February 13, 2017

Aon Benfield. (2014). *Insurance Risk Study - Growth, profitability, and opportunity*. Retrieved from http://thoughtleadership.aonbenfield.com/documents/20140912_ab_analytics_insurance_risk_study.pdf

Armenti, Lorraine A. and Cantarutti, Steven D. (21 November 2016). The Evolution of Cyber Coverage Law: A Survey of Critical Decisions and the Market's Response. American Bar Association, Retrieved from http://www.americanbar.org/publications/litigation-committees/insurance-coverage/articles/2016/fall2016-cyber-coverage.html. Last accessed February 13, 2017

Baranoff, Etti, Brockett, Patrick Lee, and Kahane, Yehudda (2009). Risk Management for Enterprises and Individuals. Flat World Knowledge Inc., Chapter 8.2.

Betterley, R. (2012). The Betterley Report: Cyber/Privacy Insurance Markey Survey 2012. *The Betterley Reportt*.

Betterley, R. (2016). Cyber/Privacy Insurance Market Survey—2016. *The Betterley Report*. Retrieved from https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf

Böhme, R. and Schwartz, G. Modeling Cyber-Insurance: Towards a Unifying Framework. In Workshop on the Economics of Information Security (WEIS). Harvard University, Cambridge, MA, 2010.

Böhme, R. Towards Insurable Network Architectures. it - Information Technology, 52, 5 (2010), 290–293.

Böhme, R. and Kataria, G. Models and Measures for Correlation in Cyber-Insurance. In Workshop on the Economics of Information Security (WEIS). University of Cambridge, UK, 2006.

Böhme, R. and Kataria, G. On the Limits of Cyber-Insurance. In S. Fischer-Hübner, S. Furnell and C. Lambrinoudakis, eds., Trust, Privacy and Security in Digital Business (TrustBus/DEXA 2006). Lecture Notes in Computer Science 4083, Springer, Berlin Heidelberg, 2006, pp. 31–40.

Business Insurance, Specialty market keeps grip on cyber risk, October 24, 2016, available at http://www.businessinsurance.com/article/00010101/NEWS06/912310137/Specialty-market-keeps-grip-on-cyber-risk, last accessed January 20, 2017.

Dearie Jr., John P. (2015). Excess and Surplus Line Laws in the United States.

Locke Lord LLP. Retrieved from http://www.lockelord.com/surpluslines/~/media/145a876771ac4edc83aea282f3aedf8a. Last accessed February 13, 2017

Ehrlich, I., Becker, G., 1972, Market Insurance, Self-Insurance, and Self-Protection, Journal of Political Economy, 80: 623-648.

Fitch Ratings. (2016, August 24). Fitch: U.S. Cyber Insurance Premiums Total $1B Per New Supplemental Filing. Retrieved from https://www.fitchratings.com/site/pr/1010744. Last accessed January 20, 2017.

Gardner, Beth (30 January 2014). Understanding the admitted and non-admitted (excess and surplus lines) insurance markets in the personal insurance marketplace. Cook Maran & Associates. Retrieved from http://www.cookmaran.com/blog/understanding-the-admitted-and-non-admitted-excess-and-surplus-lines-insurance-markets-in-the-personal-insurance-marketplace/. Last accessed February 13, 2017

Greenwald, Judy (24 October 2016). Specialty market keeps grip on cyber risk. Business Insurance. Retrieved from http://www.businessinsurance.com/article/00010101/NEWS06/912310137/Specialty-market-keeps-grip-on-cyber-risk. Last accessed February 13, 2017

Hall, S., & Robben, S. (2015). Recent Regulatory Initiatives to Tackle the Growing Threat of Cyber Risk. *Center for Insurance Policy and Research Newsletter*. Retrieved from http://www.naic.org/cipr_newsletter_archive/vol17_cyber_threat.pdf

Heal, G., & Kunreuther, H. (2003). Interdependent security. Journal of Risk and Uncertainty, 26(2–3), 231–249

Hemenway, C. (2015). ABI Research: Cyber insurance market to reach $10B by 2020. *Advisen*. Retrieved from http://www.advisenltd.com/2015/07/30/abi-research-cyber-insurance-market-to-reach-10b-by-2020/

Insurance Information Institute. (n.d.-a). Insurance Industry at a Glance. *III*. Retrieved from http://www.iii.org/fact-statistic/industry-overview

Insurance Information Institute. (n.d.-b). The Commercial Insurance Market. *III*. Retrieved from http://www.iii.org/fact-statistic/commercial-lines

Insurance Information Institute. (2017, January 24). Industry Leaders Expect Commercial Lines To Grow At Greater Pace Than Personal Lines; Cyber To Lead The Way, I.I.I. Survey Finds. *III*. New York. Retrieved from http://www.iii.org/press-release/industry-leaders-expect-commercial-lines-to-grow-at-greater-pace-than-personal-lines-cyber-to-lead-the-way-iii-survey-finds-012317

Johnson, B., Böhme, R., and Grossklags, J. Security Games with Market Insurance. In J.S. Baras, J. Katz and E. Altmann, eds., Decision and Game Theory for Security. Lecture Notes in Computer Science 7037, Springer, Berlin Heidelberg, 2011, pp. 117–130.

Kalinich, K. (2017). US Treasury Makes Standalone Cyber Insurance Policies More Valuable. Aon, January 3. Retrieved from: http://www.aon.com/attachments/risk-services/cyber/TRIA-2017Update.pdf

Markel (2017), Wholesale FAQs. Retrieved from https://www.markelcorp.com/wholesale/wholesale-faqs. Last accessed February 13, 2017

Marsh. (2013). *Benchmarking Trends: More Companies Purchasing Cyber Insurance*.

Marsh. (2015). *Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise*. March 2015.

Marsh. (2016). *Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases*. March 2016.

Morgan, S. (2015, December 20). CyberSecurity Market Reaches $75 billion in 2015; Expected to Reach $170 Billion By 2020. *Forbes*.

NAPLIA Professional Liabiity Insurance (2013). What is the difference between "admitted" and "non-admitted" insurance?. Retrieved from http://naplia.com/resources/pdf/admitted%20vs%20non-admitted%20insurance%20coverage.pdf. Last accessed February 13, 2017

National Association of Insurance Commissioners. State Insurance Regulation. Retrieved from http://www.naic.org/documents/consumer_state_reg_brief.pdf Last accessed February 13, 2017

National Association of Insurance Commissioners. (2016). Early NAIC Analysis Sheds Light on Cybersecurity Insurance Data. Washington, D.C. Retrieved from http://www.naic.org/Releases/2016_docs/cybersecurity_insurance_data_analysis.htm

National Association of Insurance Commissioners (2017). State Rate & Form Filing Review Requirements. Retrieved from http://www.naic.org/industry_rates_forms_filing_checklists.htm. Last accessed February 13, 2017

Nordman, Eric, Report on the Cybersecurity Insurance Coverage Supplement, National Association of Insurance Commissioners, 2016. Retrieved from http://www.naic.org/documents/committees_ex_cybersecurity_tf_report_cyber_supplement.pdf

PartnerRe and Advisen (October 2016) 201 Survey of Cyber Insurance Market Trends.

Price Waterhouse Coopers. (2015). *Insurance 2020 & beyond: Reaping the dividends of cyber resilience*. Retrieved from http://www.pwccn.com/home/eng/insurance_2020_sep2015.html

Rand, Jordan M. (19 January 2017). Carriers and Brokers Filling the Coverage Gap. Dilworth Paxon, LLP,. Retrieved from http://www.databreachninja.com/2017/01/carriers-brokers-filling-coverage-gaps.html. Last accessed February 13, 2017

Rand, Jordan M. (1 November 2016a). The Danger of the Cyber Endorsement. Dilworth Paxon, LLP. Retrieved from http://www.databreachninja.com/2016/11/danger-cyber-endorsement.html. Last accessed February 13, 2017

Rand, Jordan M. (18 April 2016b). Travelers v. Portal Healthcare Solutions—NBD. . Dilworth Paxon, LLP. Retrieved from http://www.databreachninja.com/2016/04/travelers-v-portal-healthcare-solutions-nbd.html. Last accessed February 13, 2017

Rand, Jordan M. (29 September 2016c). The Physical Damage Hot Potato. Dilworth Paxon, LLP. Retrieved from http://www.databreachninja.com/2016/09/physical-damage-hot-potato.html. Last accessed February 13, 2017

Rand, Jordan M. (24 February 2016d). Show Me the Money—Seriously, Because We Can't Find It. Dilworth Paxon, LLP. Retrieved from http://www.databreachninja.com/2016/02/show-money-seriously-cant-find.html. Last accessed February 13, 2017

Rand, Jordan M. (10 June 2016e). P.F. Chang's On the Hook for Contractual Liabilities. Dilworth Paxon, LLP. Retrieved from http://www.databreachninja.com/2016/06/p-f-changs-hook-contractual-liabilities.html. Last accessed February 13, 2017

Schutzer, D. (2015, February). An Assessment of Cyber Insurance. *CTO Corner*. Retrieved from http://fsroundtable.org/cto-corner-assessment-cyber-insurance/

Standard & Poor's. (2015, June 9). Looking Before They Leap: U.S. Insurers Dip Their Toes In The Cyber-Risk Pool. *Standard & Poor's*. Retrieved from https://www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1403078&SctArtId=320678&from=CM&nsl_code=LIME&sourceObjectId=9194506&sourceRevId=12&fee_ind=N&exp_date=20250609-19:35:11

UK Cabinet Office. (2015). *UK cyber security: the role of insurance in managing and mitigating the risk*. Retrieved from https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance

Where Cyber Insurance Underwriting Stands Today. (2015). *Insurance Journal*. Retrieved from http://www.insurancejournal.com/news/national/2015/06/12/371591.htm

Willis. (2014, March). That's the board and they're asking about cyber risk. *Willis Insights*. Retrieved from https://www.willis.com/documents/publications/InsightsCoverStory/50236_INSIGHTS_Publications_Mar_2014.pdf