THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF RISK MANAGEMENT

SHOULD THE PUBLIC OR PRIVATE SECTOR INSURE CYBER RISKS?

COLLEEN TYGH
SPRING 2016

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Risk Management
with honors in Actuarial Science

Reviewed and approved* by the following:

Zhongyi Yuan
Assistant Professor of Risk Management
Thesis Supervisor

Richard London
Instructor of Risk Management
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

This research explores the question of whether the United States government or the American private insurance industry is the better party to properly insure cyber risk. While businesses that purchase cyber insurance coverage can absorb some smaller losses from cyber attacks on their own, an insurance company typically covers the costs of business interruption, technological assets, customer notification, public relations, legal work, and other related expenses. In recent years, cyber security threats have grown exponentially and expanded into market segments and industries not previously protected, thereby increasing the demand for cyber insurance products with higher limits and broader coverage.

After providing an overview of cyber insurance's history and current market status, this thesis then discusses the characteristics that make a risk insurable and the emerging insurance modeling methods that may be applicable to cyber insurance pricing. Examples of insurance lines and products that are currently sold by the private insurance industry are provided to aid the analysis of that industry's ability to insure against all conceivable cyber risks. Two insurance programs run by the federal government, which can serve as models for a potential government-sponsored cyber insurance program, are also considered.

Private insurance companies have built actuarial pricing models for some cyber products. However, as cyber criminals and terrorists become more of a threat, the private sector may not be able to handle the vast liabilities that these risks pose. There is no way to accurately predict how much damage a single cyber attack could cause in the future, and thus there is no reliable way to price the associated insurance products. A temporary government reinsurance program could be established to cover losses from cyber attacks that affect many businesses and industries at the same time until the private sector feels confident that it can adequately model these risks.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

Thank you to Richard London for the all of the support and input you have given me throughout the completion of this thesis. I am truly proud of the final product thanks to all of your help.

To Zhongyi Yuan, thank you for taking the time to read this thesis and to provide your valuable commentary.

Finally, thank you to Ron Gebhardtsbauer. You have served as a professor, role model, and mentor for me throughout my four years at Penn State, and your passion for the actuarial profession has undoubtedly inspired me to pursue a successful career in the actuarial field.

Chapter 1

Introduction

Target, Home Depot, JP Morgan, Sony Pictures – all are businesses that have experienced infamous cyber attacks. Who pays for the cost of data breaches such as these? How should the economy handle something larger in scope and scale? As the world becomes smaller due to technological advances and greater interconnectedness, the need for cyber insurance becomes greater. Fifty years ago the idea of something like a data breach may have been unimaginable. Today it is impossible to define how much damage a cyber attack could cause and in what form it could occur. To analyze whether the government or private sector is better prepared to protect against cyber risks, it is useful to first examine how similar insurances have been dealt with in the past and how actuaries are currently tackling cyber products and issues. It might then be possible to decide which party can better bear cyber security risks.

Chapter 2 provides a history of cyber risk and insurance. A cyber event is first defined since it can take on different meanings by different insurers, businesses, scholars, governments, and other parties. Then the evolution of cyber attacks is described. As time passes, cyber attacks become more severe and dynamic. An evaluation of the current market for cyber insurance is provided to show what the private sector has been able to manage thus far.

Chapter 3 discusses the criteria that risks must meet to make them insurable. Although all of the insurability characteristics are desirable to insurers when looking to value a risk, not all need to be met in order for the private sector to design products covering those risks. Examples of risks that meet some or all of these criteria, and thus are widely insured by the private sector, are provided. Additionally, three recently developed modeling methods, with applications to insurance product pricing, and more specifically to cyber insurance pricing, are discussed.

Chapter 4 discusses two government-sponsored insurance programs. The first is the National Flood Insurance Program (NFIP), which was created in the 1960s when flood risk was deemed uninsurable by the private insurance industry. The other is the terrorism insurance program created by the Terrorism Risk Insurance Act (TRIA) in 2002 as a response to the terrorist attacks of September 11, 2001. The government plays a different role in each of these programs, and many experts in the cyber insurance field consider these programs as potential models for a federally run cyber insurance program.

Chapter 5 assesses whether cyber risk meets the standard criteria of an insurable risk and compares cyber risk to other risks that are commonly covered by products currently sold in the private insurance market. A proposal for a temporary government reinsurance program is then introduced. This program would allow government intervention in the case of extreme cyber events causing massive losses that the private sector cannot manage. However, as the private sector eventually becomes more capable of predicting these major losses, and thus begins to sell products covering larger cyber risks, the government reinsurance program may no longer be needed.

Chapter 2

Cyber Background

Defining Cyber Events

As forms of communication have advanced throughout history, people have grown more closely connected. The invention of the cell phone, smart phone, computer, tablet, and the modern Internet has expedited the growth of many industries and improved most business processes. However, these developments have also contributed to an increasing dependence on technology, and now almost all aspects of human life involve technology in some form. Technological systems have generated a new type of risk for businesses called *cyber risk*. Cyber risks are defined as "… the specific risks that relate to the use of computers, information technology and virtual reality."[1] Cyber risks arise from possible *cyber events*, or situations that, if they occurred, could cause a business to suffer a potentially catastrophic loss.

Considerable debate surrounds the issue of what exactly constitutes a cyber event. This discussion is especially important because the language in cyber insurance policies is often vague, and policyholders have begun to request more specific wording in these policies in order to precisely identify the events the policies cover. Most businesses purchase cyber insurance policies to cover *cyber crime* and *cyber terrorism*. Each new act of cyber crime or terrorism creates more awareness of security measures within businesses that cannot defend themselves against the technological capabilities of felons. Thus, new types of insurance coverages emerge.

Data breaches are cyber events that are commonly covered in current cyber policies. Usually, cyber criminals "… steal money or information that can eventually be monetized, such as credit card

[1] See [5], p. 3.

numbers, health records, personal identification information and tax returns."[2] The criminals will typically hack into a business's information database and steal the customers' information. Data breaches can lead to a different type of cyber event called *identity theft*. When sensitive information such as a person's Social Security number, birth date, or PIN number is in the hands of criminals, it can be used to make purchases in the victim's name. If hackers can access information databases, they likely can gain control of a business's entire information systems unit and security network as well. Business interruption will occur if the hackers alter the system or shut it down completely, and either situation would leave the business with sizable recovery costs. Operational disturbances can interfere with a business's ability to serve customers, and if the business notifies the public about a hack, it can suffer reputational damage. Thus, cyber events can directly or indirectly cause business interruption and damage to reputation.

Although cyber crimes and terrorism make up the majority of a business's cyber worries, employees can also cause a cyber event. Human error can lead to the accidental release of sensitive information. For example, human error could produce an email to unintended recipients containing personal information about customers. Another type of cyber event involves lawsuits resulting from other cyber events. These lawsuits can involve a multitude of cases, such as a business suing attackers over a copyright or trademark infringement or customers suing a business for insufficient security measures that led to their identity theft.

Cyber events can take many forms, and those mentioned above are just a few of the more common current varieties. Insurers that sell cyber insurance coverage intentionally use imprecise language in their policies because no one knows exactly what types of cyber events are possible in the future. Although businesses are wary of certain attacks because other businesses have experienced them in recent history, cyber criminals and terrorists are continually advancing their attacks and creating schemes that insurers and policyholders could not possibly preempt. As different kinds of cyber events occur and more businesses seek cyber insurance coverage, a trend toward more specific policy language

[2] See[6], par. 3.

has surfaced. A more precise definition of which cyber events are included in a policy's coverage will eliminate confusion over who is responsible for different losses resulting from cyber crimes. However, while insurers are discussing what coverages their policies will include, the business world is discussing whether the private sector is even capable of insuring these potentially monumental losses.

Cyber Attack History

The demand for cyber insurance continues to grow as businesses fall victim to cyber attacks. These attacks date back to 1988, when "the Morris worm – one of the first recognised [sic] worms to affect the world's nascent cyber infrastructure – spread around computers largely in the U.S."[3] Robert Morris, a student at Cornell University at the time, released this worm in order to privately study the true expanse of the Internet. The worm completely froze some computers when it infected them more than once and greatly slowed their processing speed. Although the computers merely needed to be rebooted in order to start working again, Morris's worm sparked a conversation about cyber security. Since then, and especially with the development of the World Wide Web and the modern Internet, many more cyber criminals have affected organizations. An insurance recovery law firm, Gilbert LLP, stated that "… 'between 2005 and 2011, there were over 2300 data breaches, exposing over 535 million records at an average cost to the affected firms of $234 per compromised record.'"[4] A list of some well-known businesses and other parties who have experienced cyber attacks in the twenty-first century is displayed in Table 1.

In 2000, a Canadian teenager who dubbed himself "Mafiaboy" on the Internet hacked into the CNN website. However, officials say that he accomplished this only by mimicking the tactics of high-profile cyber criminals. Some originally thought Mafiaboy was connected to the hacking of Amazon,

[3] See [28], par. 1.
[4] See [9], p. 204.

eBay, and Yahoo! websites as well, but these charges were dropped; some other dangerous hackers had gotten away with these three crimes. A year later, another teenager, this time from the United States, hacked into NASA's computer systems and posted pictures on their websites but did not touch any

Table 1. Notable Cyber Attacks in the Twenty-First Century

Year	Cyber Attack
2000	CNN
2001	NASA
2007	U.S. Secretary of Defense email account
2008	Republican and Democratic U.S. presidential campaigns
2008	Church of Scientology
2009	Government, financial websites, and news agencies in U.S. and South Korea
2009	Google China
2013-14	Target
2014	eBay
2014	Sony
2015	JPMorgan Chase

important information. After a few smaller, yet effective, cyber attacks in the United States and a huge multinational attack involving multiple industries, some attackers attempted to access the Gmail accounts of Chinese human rights activists in 2009. Although Google claims the hackers did not gain access, the business had to "… 'review the feasibility' of its business operations in China."[5]

All these cyber attacks spurred the United States government to take action. Early in 2013, "… President Obama signed an executive order to establish a national framework to strengthen cybersecurity … [but] this did not prevent massive data breaches such as the one experienced by the Target Corporation."[6] Many businesses did not have time to implement the new policies before new attacks occurred. Target's data breach affected at least seventy million customers due to problems with the security of the business's credit card reading system. Then, in 2014, a very prominent year for cyber attacks, cyber thieves stole customers' email addresses, passwords, and birth dates from eBay's account

[5] See [10], par. 6.
[6] See [11], p. 1.

database. The business urged all users to change their passwords immediately. In one of the most memorable cyber attacks in recent history, "in late 2014, Sony Pictures Entertainment experienced a barrage of network intrusions and disruptions, accompanied by extortionate threats."[7] These threats were connected to the planned release of *The Interview*, a satirical movie about assassinating North Korean dictator Kim Jong Un. Although the attack generated a lot of buzz about the movie and did not cause much financial loss to Sony, it embarrassed many of the business's executives and exposed their substandard risk management practices. This event also marked the first time that the United States publicly blamed a nation state, rather than a few individuals, for a cyber attack. Finally, in 2015, "three men who orchestrated a cybercrime spree made off with the personal information of more than 100 million people and generated millions of dollars in illegal profits"[8] when they attacked JP Morgan Chase. This cyber crime showed that hacking is now becoming more of a business model rather than a way to make a quick profit.

The media, and the world at large, tended to criticize the victims of these cyber attacks for poor security measures. As these businesses worked on risk management improvements, they also became more interested in purchasing cyber insurance products. Thus, insurers began developing these products and moderating them to fit with changing customer needs. As attacks have become more complex, so have the insurance products covering them.

Market for Cyber Insurance

Cyber insurance has not been a popular product until fairly recently. According to an adviser at Chernoff Diamond & Co., a benefit consulting firm based in New York, not many companies were interested in buying cyber insurance in 2012. Four years later, however, up to twenty percent of this

[7] See [12], par. 3.
[8] See [8], par. 1.

adviser's customers now buy cyber policies, primarily due to the increasing rate at which cyber attacks have occurred in the past five years. Multiple surveys within the United States have shown that approximately twenty-eight to thirty-five percent of businesses have purchased some sort of cyber insurance coverage. According to XL Group, an insurer with considerable business in the United Sates that has experienced consistently large growth in cyber insurance sales, most of the businesses purchasing these products are large and mid-sized firms. Many small businesses feel that they do not have enough data or customers to warrant cyber criminal interest in attacking them. They also see the extra insurance premium as a cost that is not worth the benefit. Some small businesses who do have cyber insurance policies have simply rolled this coverage into their general liability policies because adding additional coverage to an existing policy may cost less than purchasing a new policy.

Many businesses are very unsure of how much cyber insurance they should purchase, so they are beginning to involve insurance brokers in all aspects of the purchasing process. Brokers can help businesses understand their insurance needs, explain what products insurers are currently offering, and seek out competitive pricing. These brokers will become even more important as the United States government starts requiring companies to purchase cyber insurance policies. For example, the Securities and Exchange Commission (SEC), "… encourages publicly traded companies to give a '[d]escription of relevant insurance coverage,' and, in some situations, requires disclosure regarding past cyber attacks and future threats."[9] The White House has also produced statements about cyber insurance coverage, noting that businesses with outstanding risk management and security measures will pay lower cyber premiums. Additionally, many potential business partners have started making cyber insurance coverage a contractual requirement when making deals with other businesses.

The cyber insurance market generates approximately five hundred million dollars of premium each year and has grown between ten and twenty-five percent annually. Some insurance experts have

[9] See [9], p. 205.

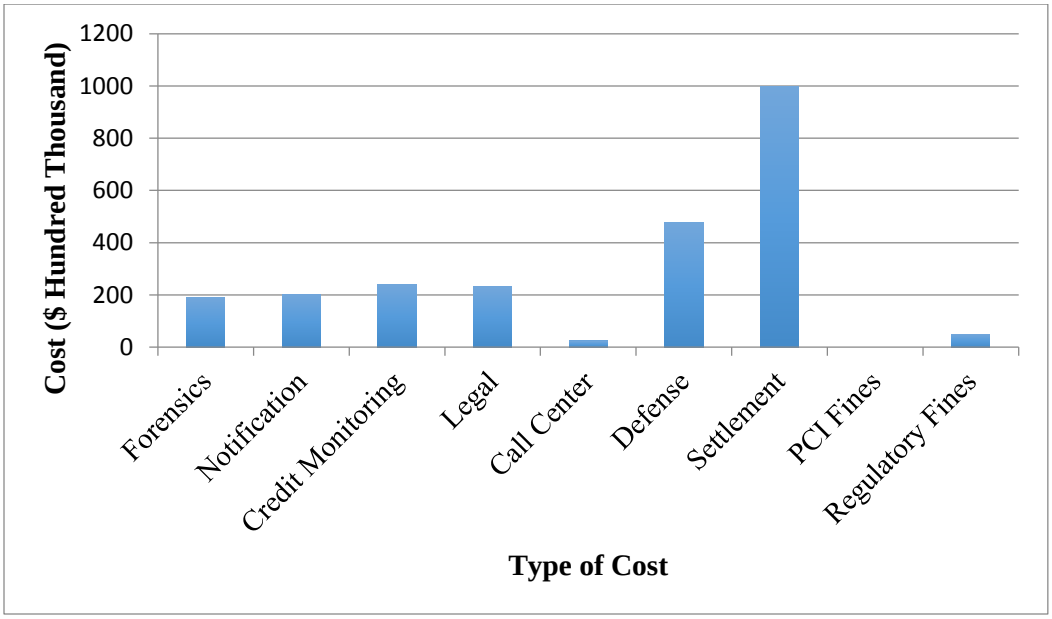
even claimed that cyber insurance is "… 'the only insurance line in a growth mode.'"[10] The principal customers are businesses involved in the retail, law, accounting, banking, and healthcare industries. Despite this insurance field's tremendous growth projections, the cyber insurance market is certainly a market of unknowns. Many insurers jumped into this new and expanding market so they would not miss out on potentially lucrative opportunities. However, most insurers did not establish sound underwriting practices for this new type of coverage, and therefore these businesses might not be prepared for future catastrophic losses. Potential purchasers of cyber insurance are just as inexperienced. Many businesses do not know how to protect themselves internally, so if they do not buy insurance or do not buy the right amount and type of coverage, they may have uninsured or underinsured losses in the future. On the other hand, many businesses place too much trust in their insurance coverage and feel they do not need strong internal security processes because the insurer will cover any losses that occur.

Over fifty insurance companies are now selling cyber insurance products, and this number is growing. These products fall into two main categories; some products cover a business if some unauthorized user accesses and exploits its computer network and systems, whereas other products cover businesses and employees that violate privacy regulations and disclose data to unauthorized parties. Many individual coverage options exist, and businesses can choose which to buy or purchase all of them as a package. These individual policies include (a) coverage for notifying customers of cyber attacks, (b) replacing or recovering data lost in an attack, (c) costs of business interruption, (d) reputation management, (e) losses from identity theft, (f) litigation and regulatory compliance expenses, and (g) forensic auditing. Figure 1 shows the average cost allocation per cyber attack as of 2013.

Insurance products currently on the market do not cover all costs resulting from cyber events. For example, businesses will not find products that cover the value of stolen intellectual property. Most policies also have exclusions and other requirements. If a business discovers that a hacker has access to its system, it cannot then decide to buy an insurance policy covering that cyber attack. Also, some insurance

[10] See [27], par. 15.

Figure 1. Average Cost per Breach (Source: Glascott)



policies require policyholders to make a reasonable effort to secure their own systems; if they do not, they will not receive coverage. Insurance purchasers should also note if their policy expressly includes physical damage. One of the most important insurance requirements is that a business needs to know what to do if an attack occurs; most recovery and settlement actions require insurer approval.

There are many reasons why businesses do not purchase cyber insurance. Many businesses, especially the smaller ones, find the policies too expensive and the deductibles too high. Since coverage is often limited, and not very clearly defined, businesses may find that the benefits do not outweigh the costs. Some organizations have reported broker issues when buying products, such as miscommunication and lack of broker knowledge, and the businesses lack the information needed to make purchasing decisions on their own. Also, according to a survey sponsored by Zurich Re, almost seventy-five percent of companies surveyed said that the Information Technology Department was primarily or solely responsible for mitigating cyber risk rather than making cybersecurity an enterprise-wide effort. While all of these factors contribute to some businesses deciding not to buy cyber insurance, the main reason seems to be a business's belief that its internal security measures are more than adequate to defend against cyber attacks. However, it is impossible for companies to foresee all the actions of cyber criminals; as an

attorney from a cyber investigation law firm noted, "'There are people out there who can beat any system. You do the best you can.'"[11] Businesses do not know exactly what types of losses they could have and thus the amount of protection they will need in the future, so cyber insurance is on its way to becoming somewhat of a necessity. While most people in the insurance world agree that cyber insurance is a trend that will continue to spread, the question still remains as to whether the private sector can handle coverage of all cyber risks or whether the government needs to intervene.

[11] See [27], par. 19.

Chapter 3

Private Sector Insurance Programs

What Makes a Risk Insurable?

One of the major debates surrounding cyber insurance, and who should administer it, is whether cyber risk is actually an insurable risk. Determining the criteria that make a risk insurable is important for several reasons. First, actuarial evaluation and decision-making tools are dependent on these criteria. Additionally, insurance regulation requires a fine and more precise definition of insurance. Most importantly for cyber insurance, however, is that new ideas for insurance products may involve coverage for uninsurable risks, so defining exactly what risks are insurable is essential.

Throughout insurance history, researchers have debated the characteristics that make a risk insurable. The list of requisites for insurability now includes, but is not limited to "(a) large number of homogeneous exposure units, (b) independence of exposure units, (c) calculable expected loss in monetary value, (d) definite loss as to time, place, amount, and cause, (e) fortuitous loss, (f) economic feasibility, and (g) avoidance of catastrophic potential."[12]

The requirements that there must be a large number of homogeneous exposure units and that those units must be independent are very much related. Exposure units differ depending on the type of insurance. For example, an exposure unit for life insurance is a person and for property insurance is a building. In order for an insurer to pool exposure units together, the units must be independent and embody the same risk. A health insurer, for instance, could pool females whose risk level is similar and

[12] See [25], p. 321.

whose chances of acquiring a certain disease remain unchanged even if another person in the pool contracts the disease, which is what is meant by independence of exposure units.

The satisfaction of these requirements enables insurers to predict future losses based on the Law of Large Numbers, which is a concept used in insurance to explain the pooling mechanism. This law "… holds that the average of a large number of independent identically distributed *random variables* [or exposure units] tends to fall close to the expected value. This result can be used to show that the entry of additional risks to an insured pool tends to reduce the variation of the average [sic] loss per policyholder around the expected value."[13] In other words, with more exposure units, the insurer's predicted loss is more likely to be closer to the actual future loss. This law also implies that with more people in the insured pool, insurers can more adequately cover future large losses because each person pays a premium but not everyone has a loss. The Appendix to this paper provides a more detailed description of the Law of Large Numbers.

Additionally, if enough exposure units do not exist, the insurer cannot be as confident about its expected loss estimations and thus must charge a higher risk premium, or amount above the expected value of the loss. If the exposure units are not homogeneous, other problems can develop. For example, if low-risk people and high-risk people are the only two types of insured groups, and if the insurer charges both groups the same premium, *adverse selection* can occur. If the risk premium is greater than the amount the low-risk group is willing to pay above the expected loss, then those people, who had been subsidizing the cost of high-risk people, will opt out of buying insurance. The insurer will be left with only high-risk consumers in its pool who are paying less than their individual group's expected loss value.

Another characteristic that makes a risk insurable is the calculability of the probability of loss. More specifically, "the insurer must be able to calculate both the average frequency and severity of future losses with some accuracy."[14] Actuarial estimates of both frequency and severity models are based on a

[13] See [26], pp. 1-2.
[14] See [23], p. 8.

lot of historical data. In fact, the Dictionary of Finance and Banking defines an insurable risk as "the possibility of suffering some form of loss or damage that can be described sufficiently accurately for a calculation to be made of the probability of its happening, on the basis of past records."[15] If insufficient data exists, actuaries will find it hard to confidently make loss estimates. Without an adequate expected loss approximation, determining the amount of premium to charge and reserves to hold is merely a guessing game. Calculability problems can also stem from unknown hazards. For example, health insurers cannot possibly estimate the probability of losses due to certain diseases that are not yet identified; "the insurability of these risks is in doubt because the value of the loss is nebulous."[16]

Insurable risk must also be associated with a determinable and measurable loss. Losses must have a definite time, place, cause, and amount so that insurers can determine if losses are covered under policies and, if so, how much they owe the insured in claims. For example, life insurance has a definite cause (death) and an amount owed that is specified in the policy. Other losses, such as pain and suffering, are far more difficult to measure.

A loss should also be fortuitous, meaning it occurs accidentally and is out of the control of the insured party. Insurable risks only refer to the random occurrence of events. There are two problems with insuring intentional losses. First, insurers could no longer accurately estimate the probability of making all future claim payouts because the pricing based on random occurrence would be unusable. Insuring intentional losses would also lead to high moral hazard. For example, the beneficiaries of life insurance policies might have a motive to murder the policyholder in order to receive the benefits. A less extreme example of moral hazard occurs when policyholders fail to act in a manner that could prevent loss, whereas they do act more cautiously when their loss is not insured.

Economic feasibility is another concern regarding the insurability of risks. Administrative fees and other expenses accompany policies that insure small losses occurring with reasonably high

[15] See [19], par. 1.
[16] See [25], p. 324.

probability. These risks are typically deemed uninsurable because the amount of premium is high compared to the amount of covered loss. Pooling does not occur; each insured party pays its own losses, plus a percentage of the insurer's expenses. Since the losses are small, most people and businesses choose to self-insure them. A low probability of loss is especially key to a risk's insurability. People who are ninety-nine years old have a hard time finding an insurer who would sell them life insurance because the probability of death in the near future is very high at that age. They would either need to pay a large premium, almost equal to the amount of the benefit itself, or pay a more affordable premium but expect little benefit.

The last characteristic of insurable risks is the avoidance of potentially catastrophic losses. If all the other characteristics of insurability are met, this last requisite is met by default. Catastrophic events have the potential to effect a large portion of an insurer's business. For example, a hurricane that makes its way along the entire eastern coast of the United States could trigger claims from many of a business's property insurance policyholders. Insurers have different means of protecting themselves from catastrophes. They may transfer a portion of the risk to third parties via catastrophe reinsurance or catastrophe bonds, and these third parties can similarly transfer risk to additional parties, helping to spread the overall risk across a larger capital base relative to the primary insurer. Additionally, insurers diversify their risk by building geographically dispersed business so that a single, geographically dependent peril is less likely to affect the insurer's overall results.

Table 2 shows whether four risks meet the various aforementioned insurability criteria and shows if the private insurance sector currently underwrites these risks. As shown in red in the table, many insurance products exist today covering risks that do not meet all of the criteria. If a certain criterion is not met, the insurance policy usually includes different provisions and conditions. Whether or not cyber risk meets these criteria is an important aspect of the debate regarding who should insure it.

Table 2. Insurable Risk Examples (Source: Park)

Insurability Characteristic	*Flood Risk*	*Fire Risk**	*Disability Risk*	*Terrorism Risk*
Large number of similar exposure units	Yes	Yes	Yes	No
Accidental, uncontrollable	Yes	Yes	Yes	No (man-made, but not by insured)
Potentially catastrophic	Yes	No	No	Yes
Definite losses	Yes	Yes	No	Yes
Determinable probability distribution of losses	Yes	Yes	Yes	No
Economically Feasible	Not always	Not always	Not always	No
Insurable?	**NO**	**YES**	**YES**	**NO**

*Excluding fire following an earthquake, which could be catastrophic

Private Insurance Examples

In order to determine whether the private sector can handle cyber insurance, an analysis of other insurance programs managed by the private sector will be helpful. The most common of these programs are life insurance, health insurance, property-casualty insurance, and catastrophe insurance. All of these coverages have specific characteristics that are important to our discussion about cyber risk insurability.

Life insurance policies specify the amount of money to be paid when the insured dies, as well as the beneficiary who will receive that money. Defining the risk is not difficult for whole life insurance because death is certain to occur for all insured people; the time of death is the only risk that the insurer faces. Life actuaries estimate the probability of death at different times in the future but do not have to estimate the severity of the loss, which is defined in the policy. These certainties make life insurance an easy product for the private sector to administer. The same cannot be said, however, for cyber insurance products.

Another characteristic of life insurance is that people are not always aware of their need for it. Although the risks are insurable, insurers and their agents must actively sell their products. Sales volumes

must remain controlled, however, because the policies involve upfront expenses that are much higher than expenses in renewal years. Instead of charging a very high premium in the first year of policy life only, some insurers charge moderately high premiums in the first few years of policy life to make it more affordable for consumers. However, they then run the risk that the policyholder dies shortly after the policy's inception, so they must ensure they have enough reserves to stay true to their promised payouts. The potentially long duration of a policy is a distinctive quality of life insurance that could potentially carry over to cyber insurance as well.

Health insurance is a topic that United States political figures debate vigorously, arguing about how much control the government should have over the healthcare financing system. In the United States and other countries without a universal healthcare system, "… health insurance is commonly included in employer benefit packages and seen as an employment perk."[17] According to the Center for Disease Control and Prevention in 2012, a majority of Americans have some kind of private health insurance coverage. The United States public health programs include Medicare, which provides coverage to people over age 65, and Medicaid, which provides coverage to low-income citizens. The Affordable Care Act, which President Obama signed into law in 2010, mandated that all Americans have health insurance, but healthcare regulation and laws could change in the future. The better party to insure cyber risk might become one of the next topics that Congress debates.

Property-casualty insurance covers a range of risks, typically divided into two main areas: protection for physical items (property) and protection against legal liability (casualty). Property insurance, such as covering the cost of replacing someone's house after fire damage or the cost of repairing a car that the policyholder damages, is known as "first-party" coverage because it covers only losses related to the policyholder's own property. Casualty insurance, on the other hand, is "third-party" coverage because it protects the policyholder from paying damages that he or she has caused to other parties. Property-casualty insurance can be further categorized as personal lines, which insurers write for

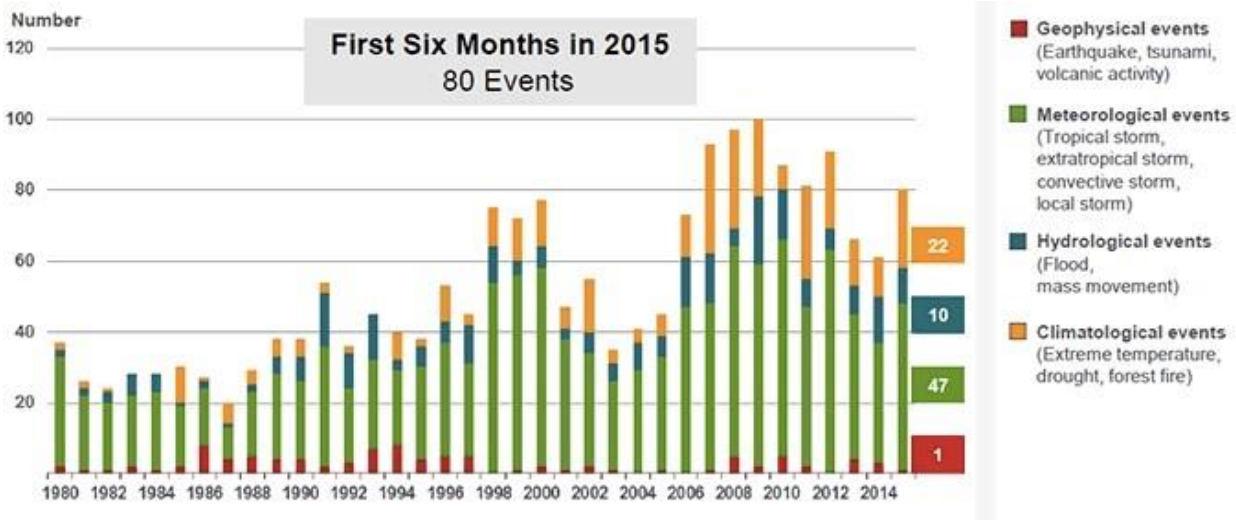
[17] See [21], par. 3.

individuals and families, or commercial lines, which insurers write for businesses. The risks that property-casualty insurance cover are certainly insurable, but these insurers have an array of both tangible and intangible risks to consider and thus a number of different products to develop. Insurers who sell cyber insurance also have an expansive list of potential coverages to consider.

As shown in Figure 2, the number of catastrophes has increased in recent years. The world is becoming more interconnected, and these catastrophes now have the potential to affect more people and business operations than ever before. When insurers first tried to model natural catastrophes, they struggled with the unpredictable nature of the events. Insurers now have much more data to work with, and "this understanding has flowed into hazard maps, construction standards, pricing models and emergency planning programmes [sic], and, consequently, a steadily increasing demand for insurance against natural catastrophes has been met by a rising willingness of insurers to cover such risks."[18] Insurers have also identified certain trends, such as climate change, that they expect to continue in the future. These trends are built into pricing models to make them more thorough and predictive. Additionally, companies such as Risk Management Solutions (RMS) and AIR Worldwide, whose primary purpose is to develop catastrophe models, can provide these models to insurers, reinsurers, and governments. Natural catastrophe risk is similar, in many aspects, to cyber risk, so catastrophe modeling may be a good starting point for actuaries trying to predict the occurrence of cyber attacks.

[18] See [4], p. 90.

Figure 2. Number of Catastrophic Events by Year (Source: Insurance Information Institute)



Emerging Modeling Methods

Researchers in the insurance industry have suggested some methods that insurance company actuaries could build into the models they use to price cyber insurance products. Using these methods, they claim that actuaries might feel more confident that the prices they calculate are adequate to cover insurers' future claim payments. Some insurers use these modeling methods, or parts of the theory behind them, to price some of the products they currently sell. Among these methods are (a) extreme value analysis, (b) the use of copulas, and (c) the use of matrices to model networks.

Researchers have been studying the application of extreme value analysis to catastrophe modeling since the late twentieth century. Risk managers at insurance companies around the world have struggled to accurately predict extreme events like natural disasters, financial crises, and large-scale crimes, and modeling these events is crucial to the solvency of the insurers. The probability of these events occurring is very small relative to the probability of less severe losses, so they fall in the very high quintile regions of a risk's probability distribution. Although time series analysis can help with some predictive modeling analytics, extreme events are usually outliers when grouped with losses of a less catastrophic nature and

thus must be dealt with separately. Analyzing these outliers separately is a common method that actuaries use to model catastrophic events. Without removing outliers, they would need "… to study quartiles and tail probabilities, which are unobservable if [they] are analyzing normal datasets."[19]

The basic purpose of extreme value analysis is to truncate a loss probability distribution to exclude extreme values, and then model the very severe, yet rare, catastrophic events separately from the less severe, but more probable, events. Once the extreme values are truncated from the dataset, the probability distribution is estimated in one of two ways, but the mathematics involved in both approaches is quite complex. Some researchers think that analyzing extreme values of cyber risk distributions could help "… control the hierarchical organization of the classes of risk … and establish reserves to cope with these extreme risks."[20]

Others in the insurance world suggest using the emerging copula methodology to model cyber risk. A copula is essentially a multivariate probability distribution with uniform marginal distributions. For insurer losses, the multivariate distribution represents the total dollar amount of loss, which depends on the number of policyholders who file claims and the amount of each claim. Each of these factors has its own probability distribution, called a marginal distribution, which are then combined to form the multivariate distribution for the total dollar amount of loss. Some insurers argue that copulas, which model dependence structure, can be used in conjunction with marginal distributions that model the size of losses in order to model the joint loss distribution. This technique is useful for risks that can have a variety of distributions. Additionally, "… copulas are ideal for investigating non-linear type dependencies that arise when non-normal marginal distributions of the type for [frequency] and [severity] are combined."[21] In other words, copulas allow the individual pricing variables to be partially dependent on each other. For example, if a business has a commercial auto policy covering a fleet of cars, and some of these cars get in a massive traffic accident, the business's claim under that policy would have a severity

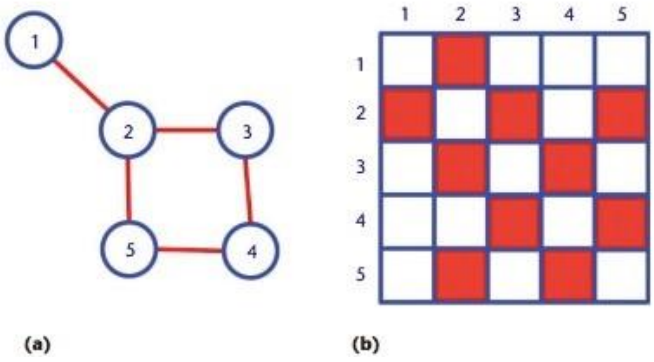
[19] See [16], p. 124.
[20] See [35], p. 249.
[21] See [14], p. 9.

dependent on the number of cars involved. Modeling the joint frequency and severity distribution for cyber risk might be more accurately predictive with the incorporation of copulas, given that cyber losses could be interdependent and quite complex.

Another modeling method emerging in the insurance world is the use of matrices to represent networks. The risk of some losses can increase when a similar loss occurs if the sources of loss are interconnected. Some describe this as the domino effect; not all losses, and thus not all policies' risks, are independent. These connections are typically represented by a *node-link graph*, as shown in Figure 3(a). The nodes, or numbered circles, represent a single policy's risk. The links, or lines connecting the nodes, show which risks are related to others. For example, a loss under Policy 2 could directly trigger a loss under Policies 1, 3, and 5, but not Policy 4 because there is no line connecting Node 2 to Node 4. Figure 3(b) shows the corresponding adjacency matrix, with the red boxes representing the related risks. This matrix can be rewritten as a regular matrix with the white boxes as zeroes and the red boxes as ones. In this numerical form, the matrix can be incorporated into loss models.

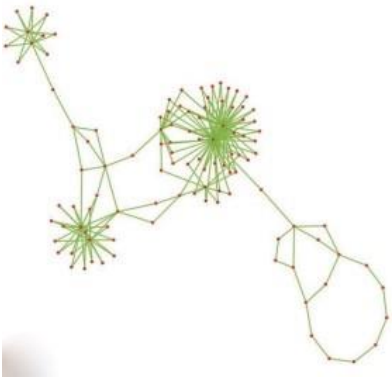
Matrices representing networks have many uses. Militaries and defense strategists can use matrices to represent the known terrorist connections and locations. Terrorism insurance also has matrix applications. If terrorists attack a certain building, for example, other businesses may be affected as well. This information would be helpful to an insurer to see which policyholders may have losses if another policyholder is subject to an act of terrorism. Some node-link graphs representing multiple network

Figure 3. Node-Link Graph and Matrix Network Representation (Source: Wong)



connections can look as complicated as the graph in Figure 4. The corresponding matrices would be equally large and complex. Many cyber insurance researchers have found parallels between the interconnectedness of terrorist attacks and cyber attacks and believe matrices can be helpful with the pricing of the respective insurance products.

Figure 4. Complex Node-Link Graph (Source: Wong)



Chapter 4

Government-Backed Insurance Programs

National Flood Insurance Program

In the United States, floods are some of the most costly natural disasters. The nation is geographically diverse, and thus exposed to a variety of hydro-meteorological hazards that cause damage to human life, economies, and ecosystems. As catastrophes such as hurricanes and snowstorms have increased in number and intensity, they have left even more flooding in their wake. American policymakers are especially concerned with this trend "… because more than half of the U.S. population now lives in coastal watershed counties or floodplain areas and approximately 50% of the nation's gross domestic product … is generated in those Gulf and Atlantic coastal areas."[22] In the second half of the twentieth century, flood hazards were deemed uninsurable for three reasons. First, adverse selection occurs when the only people buying insurance are those who live in areas likely to get flooded. Purchasing insurance would not be economical for people whose homes are unlikely to be flooded, so the insurers would not have enough low-risk people in the pool. Second, the premiums based on expected loss would be too expensive for the average single household to afford. Third, if a catastrophic flood occurred, insurers would not be able to guarantee payment based on the premiums they would be collecting.

For the three reasons listed above, most homeowner policies did not include flood insurance. In response to the growing concern over flood hazards, Congress created the National Flood Insurance Program (NFIP) through the National Flood Insurance Act of 1968. The nation seemed satisfied with this

[22] See [18], p. 4.

program at its inception. It seemed that Congress took an appropriate action to meet their responsibility to promote economic growth under the "general welfare" and "interstate commerce" clauses of the Constitution. People believed that social and ethical values should be reflected in the economy's operations, so as floods became a widespread threat, people supported shifting the risk to government so that people who were economically stressed or dislocated due to floods could receive help. The insurance world also realized that private insurance markets could not sufficiently cover catastrophic floods.

Under NFIP, "federally backed flood insurance was made available to home and business owners in communities that voluntarily agreed to adopt and enforce floodplain management ordinances designed to reduce flood-related property losses."[23] The government has major responsibilities under this program. They must identify and map flood-prone regions of the country and provide insurance to homeowners and businesses at affordable rates or with premium subsidies. They also aim to create new regulations that will reduce flood hazard risk in the long term. While NFIP protects flood victims, it also ensures that people and businesses choosing to locate in flood-prone areas maintain some degree of risk. Additionally, the program can borrow from the U.S. Treasury in case of deficits.

NFIP has changed and strengthened some of its provisions in response to more recent significant flood events. In 1973, Congress passed the Flood Disaster Protection Act, which requires home and business owners to purchase insurance for buildings located in a Special Flood Hazard Area (SFHA). The Federal Emergency Management Agency (FEMA), the organization that administers NFIP, identifies these SFHAs. Shortly after this act was established, NFIP required federally regulated lenders "… to require flood insurance on any loan secured by improved real estate in a FEMA-designated SFHA in a participating community."[24] After a 1993 flood in the Midwest, the National Flood Insurance Reform Act was passed in 1994 to enforce better lender compliance. A decade later, the Flood Insurance Reform Act of 2004 was established in response to the recognition of locations prone to repetitive flooding and their

[23] See [18], p. 8.
[24] See [18], p. 9.

financial impact on NFIP. This act created a pilot program for these severe repetitive loss properties (SRLPs) involving mitigation activities.

The program needs to be continually evaluated and reformed in light of the nation's flood-related natural disasters and NFIP's financial solvency status. Table 3 shows the largest flood events between 1978 and early 2011 according to the amount NFIP paid to its policyholders. RMS, a catastrophe modeling company, predicts that by 2030, flood losses will increase by eighty percent along the Atlantic and Gulf coastlines. As shown in Figure 5, the flood events caused by Hurricane Katrina in 2005 led to an NFIP deficit, and thus the program now has some debt to repay to the U.S. Treasury. If losses increase eighty percent, as RMS predicts, NFIP will suffer major financial problems if they do not raise premiums sufficiently.

Table 3. Top 15 Significant Flood Events Covered by NFIP (Source: King)

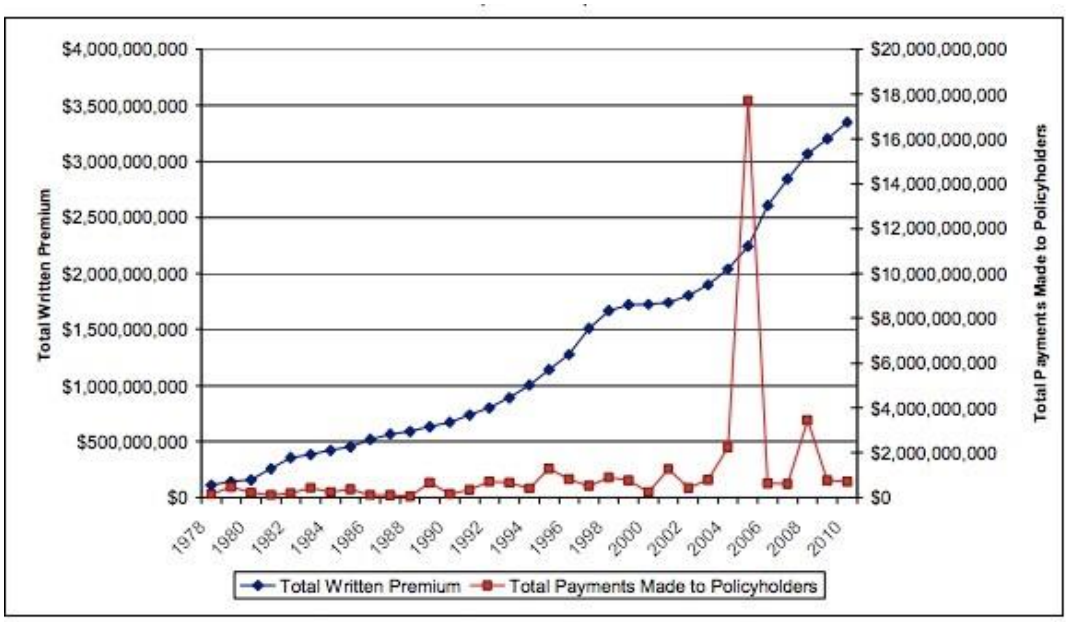
(1978 – February 28, 2011; $ nominal)

Rank	Event	Date	Number of Paid Losses	Amount Paid	Average Paid Loss
1	Hurricane Katrina	Aug. 2005	167,216	$16,172,136,626	$96,714
2	Hurricane Ike	Sept. 2008	46,219	2,629,409,589	56,890
3	Hurricane Ivan	Sept. 2004	27,637	1,582,348,735	57,255
4	Tropical Storm Allison	June 2001	30,6632	1,103,877,235	36,000
5	Louisiana Flood	May 1995	31,343	585,071,593	18,667
6	Hurricane Isabel	Sept. 2003	19,860	492,830,017	24,815
7	Hurricane Rita	Sept. 2005	9,504	470,413,959	49,496
8	Hurricane Floyd	Sept. 1999	20,438	462,268,248	22,618
9	Hurricane Opal	Oct. 1995	10,343	405,527,543	39,208
10	Hurricane Hugo	Sept. 1989	12,840	376,433,739	29,317
11	Hurricane Wilma	Oct. 2005	9,609	363,798,528	37,860
12	Nor'Easter	Dec. 1992	25,142	346,150,356	13,768
13	Midwest Flood	June 1993	10,472	272,819,515	26,052
14	PA, NJ, NY Floods	June 2006	6,410	227,475,398	35,488
15	Nor'Easter	Apr. 2007	8,639	225,623,333	26,117

Source: U.S. Department of Homeland Security, Federal Emergency Management Agency.

NFIP is currently on the high-risk list of the 2015 United States Government Accountability Office (GAO), which is renewed every two years to identify government agencies and programs financially at risk or in need of transformation. After another huge hurricane in 2012, the program's debt previously incurred from Hurricane Katrina grew even more, and the program's ability to cover future

Figure 5. Total Premiums vs. Total Payouts Under NFIP: 1978-2010 (Source: King)



Source: U.S. Department of Homeland Security, Federal Emergency Management Agency.

catastrophic losses suffered drastically. Although the Biggert-Waters Flood Insurance Reform Act of 2012 included many provisions to help the program's financial solvency, the 2014 Homeowner Flood Insurance Affordability Act "reinstated certain premium subsidies and slowed down certain premium rate increases that had been included in the Biggert-Waters Act."[25] The GAO recommends that FEMA should continue to take steps to modernize the administration of NFIP in order for the program to be removed from the high-risk list.

Members of the government and insurance industry have suggested a few policy responses to the financial problems of the nation's flood insurance program. First among these is the reform and modernization of NFIP. One possible change to the program is the implementation of new floodplain management regulations that restrict the construction of buildings in high-risk areas, and/or require new buildings in floodplains to be elevated. Another popular proposal is to phase in more actuarially based premiums for commercial buildings and incentivize more businesses to purchase flood insurance through

[25] See [15], par. 2.

the program. Others suggest that the U.S. Treasury forgive all or most of NFIP's debt. Additionally, NFIP could create a catastrophe reserve fund used only for responses to extreme flood events. Another suggestion for revamping NFIP is the creation of community group flood insurance policies. All residents of a FEMA-designated SFHA would contribute to the purchase of a group policy through property taxes or as a utility payment.

Those who oppose modernization of NFIP have proposed that flood insurance be shifted back to the private sector. Many private insurers now argue that "with the development of computer simulation catastrophe risk models and remote sensing technologies, … flood hazards are now insurable by private companies working in partnership with the government."[26] This alternative would allow FEMA to require private insurers to offer flood insurance at loss-based prices, with the federal government providing reinsurance. An idea that strengthens the argument for privatization is the creation of long-term flood insurance contracts (LTFI). Insurers need to receive premiums for a longer period of time if they wish to determine premiums based on expected losses. This method would be possible if private insurers sold five- to twenty-year policies paired with mitigation loans tied to the mortgages of insured properties. The loans would help property owners afford the high upfront costs of mitigation actions such as the elevation of buildings. The insurance policy term would be the same length as the mortgage and would continue if the owner sold the property before expiration of the policy. The debate about the future of private flood insurance and NFIP parallels the recent discussion surrounding the administration of cyber insurance.

Terrorism Risk Insurance Act

Prior to the terroristic attacks against the United States on September 11, 2001 (9/11), terrorism insurance was generally included in commercial insurance policies at no additional cost. After the events of 9/11, however, a debate ensued about whether this risk was insurable by the private sector due to the

[26] See [18], p. 24.

immense losses of 9/11, which are estimated to be about twenty-four billion dollars. As shown in Table 4, 9/11 was the second most costly "catastrophic event" in United States insurance history. Insurance and reinsurance companies were unaware of how to price policies and treaties for such unforeseeable future risks because "… they did not have historical data on similar attacks, and relevant models for such losses did not exist."[27] Reinsurers withdrew from the terrorism insurance markets, and primary insurers then found it impossible to offer terrorism coverage. This, in turn, affected many industries such as "… the real estate, transportation, construction, energy, and utility sectors."[28] Many worried that the lack of terrorism insurance would single-handedly destroy the United States economy.

Table 4. Ten Most Costly Catastrophes in U.S. History (Source: Willis)

Rank	Date	Event	Insured Property Damage (2013 $ billions)
1	August 2005	Hurricane Katrina	$47.6
2	September 2001	Fire, explosion: World Trade Center, Pentagon terrorist attacks	$23.9
3	August 1992	Hurricane Andrew	$23.4
4	October 2012	Super Storm Sandy	$19.0
5	January 1994	Northridge, CA, earthquake	$18.0
6	September 2008	Hurricane Ike	$13.4
7	October 2005	Hurricane Wilma	$11.9
8	August 2004	Hurricane Charley	$8.9
9	September 2004	Hurricane Ivan	$8.5
10	April 2011	Flooding, hail, wind, and tornadoes that struck Tuscaloosa, AL, and other locations	$7.5

The losses of 9/11 pushed the capacity limits of the private insurance market, and policies covering the risk of future terrorism attacks seemed nearly impossible to price. Most parties agreed that government intervention was necessary, but not everyone agreed on just how far they should intervene. While some called for a total government takeover of terrorism insurance, others argued that a federally

[27] See [32], p. 2.
[28] See [32], p. 2.

run terrorism insurance program should only be a temporary means of protecting against future terroristic risks.

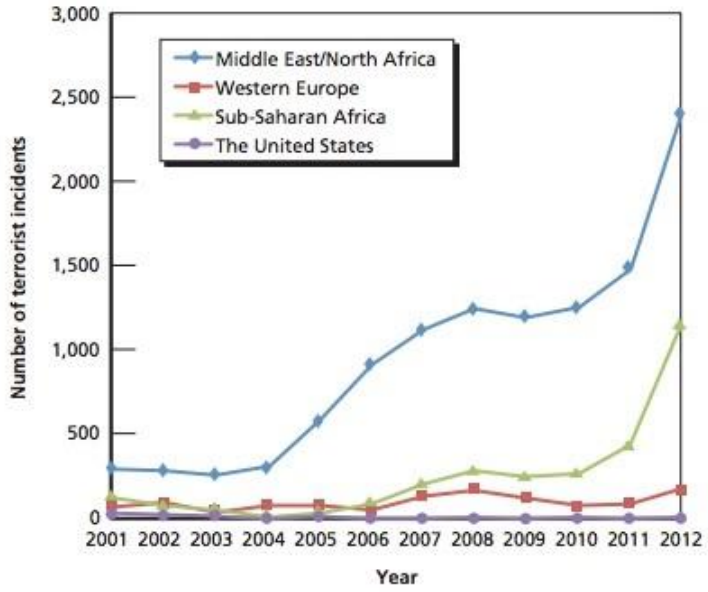
Congress seemed to agree that federal intervention should only be temporary. They passed the Terrorism Risk Insurance Act (TRIA) in 2002, "… which provided a government reinsurance backdrop in the case of a terrorist attack by providing mechanisms for avoiding an immediate drawdown of capital for insured losses or possibly covering the most extreme losses."[29] The act specifically provided some coverages, such as business interruption and commercial property damage, but explicitly excludes other insurance lines such as flood, reinsurance, and mortgage guarantees. It determined a threshold that losses must meet in a terrorist attack in order for the federal government to make payments to private insurers. Additionally, it placed a $100 billion limit on all insured losses from terrorism attacks and provided means for the government to gain back some of the money it pays out. TRIA has since been extended and reformed three separate times – in 2005, 2007, and 2014. It is now set to expire in 2019. In order to determine if TRIA should be extended, researchers are currently analyzing the pace of terrorism and the predictability of modern terrorism models.

According to the National Consortium for the Study of Terrorism and Responses to Terrorism (START), "… only 31 out of 158 sovereign nations have not experienced a terrorist attack since 2001."[30] As shown in Figure 6, there has been a sharp increase in terrorism in the past ten years in the Middle Eastern and African regions while the number of attacks has remained consistently low in the United States and Western Europe. Interestingly, most terrorism in the United States takes the form of arson committed by environmental groups who do not seek to cause human harm but instead wish to send a political message. Although al Qaeda attacks make up a small portion of terroristic attacks in the United States, they deserve special analysis. Most of the data for these attacks come from attacks that al Qaeda planned but were foiled. Al Qaeda has ties to other terroristic groups in the Middle East and Africa, and

[29] See [33], p. 1.
[30] See [33], p. 4.

many individuals who carry out terrorist attacks are also found to have connections to these same groups. Therefore, to analyze the true threat of these groups, researchers look overseas. In general, experts agree that "the possibility that in the future terrorists will attack the United States with greater frequency or more extreme methods cannot be ignored."[31]

Figure 6. Global Terrorist Attacks, 2001 – 2012, by Region (Source: Willis)

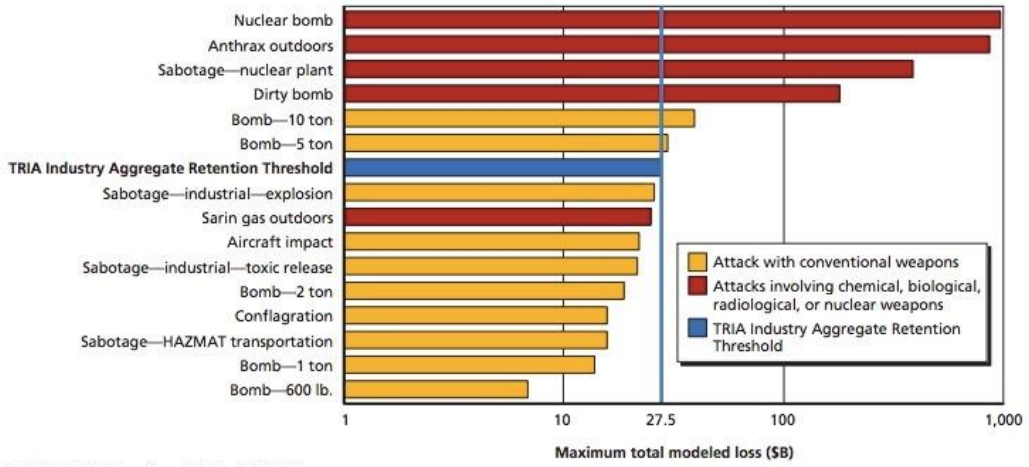


Terrorism risk is incredibly difficult to model because terrorists' intentions and decisions are completely unpredictable. In the past ten years, data has been collected on a fair number of attacks; most of these attacks are similar in nature and have fallen below the TRIA-triggering threshold. This information suggests that terrorism risk is becoming a risk that can be modeled. Experts believe these same types of terrorist attacks will occur in the future because studies have shown that terrorists often learn from each other and prefer to continue methods they know have worked in the past, rather than taking a novel, riskier approach. However, the United States must be wary that new and unconventional terrorist attacks are entirely possible and should not be overlooked. RMS has modeled the maximum total possible losses from sixteen terroristic scenarios; these losses are show in Figure 7. The results show that

[31] See [33], p. 9.

most total losses from conventional terrorist attacks will not exceed TRIA's Industry Aggregate Retention Threshold. If total losses do not exceed this threshold, the federal government is not permanently responsible for the cost of those terrorist attacks because they take back more than one hundred percent of the payouts they provide through surcharges on insurance policies across the nation. On the other hand, total losses from unconventional attacks tend to fall above the threshold, so TRIA's threshold and RMS's scenario modeling determine which types of terrorism risks cannot be modeled. If similar scenario modeling for cyber terrorism is possible, people in the insurance world discussing whether cyber terrorism risk is insurable may be interested in seeing those models' results.

Figure 7. Estimates for Maximum Attack Scenario Total Modeled Loss (Source: Willis)



SOURCE: RMS Terrorism Risk Model, 2013.

Chapter 5

Discussion

Insurability of Cyber Risk

The features of cyber risk that determine its insurability are very important for actuarial decision making and the development of pricing tools for insurance products covering those risks. These characteristics include (a) a large number of homogeneous exposure units, (b) independence of the exposure units, (c) calculable expected loss in monetary value, (d) definite loss as to time, place, amount, and cause, (e) fortuitous loss, (f) economic feasibility, and (g) avoidance of catastrophic potential.

For an individual insured, the exposure unit could be the number of customer accounts, because this highly influences the size of the loss resulting from a data breach or other cyber event. However, when examining an insurer's ability to price cyber insurance according to the Law of Large Numbers, we think of the exposure units as the insured businesses themselves. This is similar to the individual auto insurance market in which actuaries consider the individual car the exposure unit. The number of total customer accounts under all insured companies combined cannot satisfy the Law of Large Numbers requirements because not all customer accounts have independent risks. For example, if an insurer sold a cyber insurance policy to just one business that had even a billion customer accounts, that very large number of accounts would not satisfy the Law of Large Numbers requirements because the individual accounts' risks of loss from cyber events are not independent of each other. If a cyber attacker acquires information from one of those accounts, it almost certainly can get access to every other customer account as well. Therefore, the insurer must sell policies to many different insured companies to create a risk pool in accordance with the Law of Large Numbers. The number of insured companies must satisfy the "large" requirement, not the number of total customer accounts. Even with a book of business comprised of many

insured companies, however, independence is questionable. If multiple insured companies use the same service provider for their security networks, for example, a hacker accessing one business's networks can access the networks of the others as well.

To determine whether the insurer's expected loss is calculable in monetary value, classifying and grouping the insured companies is essential. This classification is where the number of customer accounts for each insured comes into play. A business with more customer accounts may be a bigger target for attackers and thus a larger risk for the insurer. Other classifying variables might include sales and credit score. Sales can help determine the losses resulting from business interruption due to a cyber attack, and credit score may provide insight into the strength of a business's risk management practices and thus its cyber risk level. By grouping insured companies with a similar risk level, actuaries can model each group's frequency and severity distributions. They can then use these distributions to predict each group's expected loss.

The use of these classifying variables has certain limitations. If two insured companies use the same security network provider, their risk of loss is correlated. If they are classified in different groups according to number of customer accounts, for example, these classifications no longer provide a strong representation of risk level because one group's loss could be related to the other group's risk of loss. Also, actuaries may classify the insured companies into different groups but have no way of knowing which groups are riskier. One could assume that a lucrative, multinational business with millions of customers is more at risk than a small business with one location and only hundreds of customers. However, actuaries have no way of knowing definitively that cyber criminals want to attack larger targets.

Another issue with the insurability of cyber risk is the lack of historical data on cyber attacks and their resulting losses. Since cyber attacks are relatively new events, actuaries cannot rely on past attacks to predict the loss amounts from similar attacks in the future. For other insurance products, such as individual auto insurance, actuaries use historical accident data to price the products sold today. For example, the actuary would price the policy for a teenage boy according to the historical losses of other

teenage boys with similar risk levels. With a lack of recorded cyber attack losses from the past, actuaries must find other methods to price cyber products. Although some historical data on cyber event losses are available through company reports and the U.S. Securities and Exchange Commission filings, companies who are victims of smaller-scale cyber attacks prefer not to publicly announce these attacks for fear of damaging their reputations. Acquiring sufficient historical data would be a good first step in pricing cyber insurance products, but "'because cyber risk is both growing and rapidly evolving, information about the past may be of limited predictive value when looking at the future.'"[32]

Unlike losses experienced with life insurance, with its definite amount and cause, losses from cyber crimes cannot be definite with respect to time, amount, place, and cause. No one can be sure what cyber criminals are thinking and scheming. Although experts in the cyber world have identified some conventional methods that hackers use, many unknown hazards could emerge. Just as health insurers cannot predict losses from a disease not yet discovered, cyber insurers cannot predict the losses from cyber crimes conducted with methods never before seen. One cyber insurance researcher "… likened the situation to making a side bet on a contest, one between the business and the attacking hackers. One of the parties – the insured – you know well. The other side, however, resembles 'a cage match where anyone can enter the ring.'"[33] Also, as companies innovate, they introduce new vulnerabilities. Each new technological process is susceptible to cyber attack, so as companies innovate they must develop additional methods of protecting the new technology.

Losses from cyber risk can be considered fortuitous. Although the cyber criminals intentionally access companies' networks, the insured companies themselves do not purposefully expose themselves to cyber attacks. Cyber risk also meets the requirement of economic feasibility. The losses can be large, but they occur with a low probability. Some argue that cyber risk is uninsurable, however, because of its potential for catastrophic loss. This is the biggest issue with cyber risk's insurability, especially as

[32] See [1], p. 38.
[33] See [20], p. 43.

researchers discover that cyber terrorism and cyber attacks affecting multiple companies are becoming increasingly realistic. These extreme events can affect many businesses and industries, thus affecting the economy as a whole. For example, losses from the terroristic attacks of 9/11 devastated many industries and required government intervention, and an act of cyber terrorism could have similar results. Therefore, actuaries pricing cyber insurance products tend to add large risk premiums to account for the uncertainty of cyber attacks, just as flood insurers did before Congress created NFIP. The higher risk premium may make cyber insurance unaffordable for some businesses.

Having a geographically dispersed book of business does not diversify risk as it does for catastrophe insurance lines such as property insurance for damages from a hurricane. Technological systems and devices are extremely interconnected today, so the location of a cyber attack is irrelevant. Although primary insurers can purchase reinsurance, companies looking to buy cyber insurance will find that most insurers selling cyber products have relatively low limits in place.

However, although cyber risk does not meet all the criteria making a risk insurable, it is not necessarily uninsurable by the private sector.

Proposal

A temporary government reinsurance program could ensure that the private sector remains responsible for a majority of cyber risk, while also addressing the aspects of cyber risk that make it seem uninsurable. The program would essentially create a government funded catastrophic response to cover severe cyber losses. Congress would have to renew the program every few years until it feels that the private sector can handle larger cyber losses on its own, and with each renewal, it could reform the program to consider any issues or solutions that have emerged since the last revision. With increasing probability that larger attacks producing larger losses will occur in the future, insurance and reinsurance companies may be interested in shifting more risk to the government. Until more extreme cyber attacks

occur, and the private insurers and reinsurers know what types of losses they must deal with, it would be hard for them to sell products at a premium affordable to companies but sufficient to cover the risk of catastrophic losses.

Like the program created by TRIA, this program would create a threshold that determines which losses require the government to step in to help the insurer and/or reinsurer. If a single insurer or reinsurer loss from one cyber attack surpassed the threshold, the government would provide financial aid to them by taking responsibility for all claims above the threshold. Therefore, the private sector would handle most cyber insurance claims, and the government would only get involved when extreme, more unpredictable events occur. For example, a cyber terrorism attack might knock out the nation's entire power grid, and the private insurance market would not be able to handle all the resulting losses. The government might also intervene if a cyber hurricane occurs, which is a cyber security event that spreads to a multitude of companies within a limited timeframe. The government reinsurance program would also likely have a limit on the total amount of financial aid it can provide for one cyber attack, similar to that of the terrorism insurance program created by TRIA.

While the government reinsurance program exists, it would have responsibilities other than providing financial aid to the private sector. The program would collect data on all cyber attacks that affect companies in the United States and release this information to insurance and reinsurance companies for use in pricing their products. The program administrators could also study the characteristics of companies that make them more likely targets to cyber criminals and create a map that shows how companies' networks and technological programs are interdependent and related. They could develop a list of best security practices that make companies less likely to fall victim to cyber attacks. Additionally, and similar to NFIP's "severe repetitive loss" properties, they could identify "severe repetitive loss" security networks or technological systems that insurers could reference when pricing products. If insured companies use these high-risk technologies, insurers can charge them higher premiums. The program could also provide mitigation loans. Companies that want to purchase cyber insurance will pay a lower

premium if they have better risk management strategies and technological systems. The implementation of these practices can have high upfront costs, and these mitigation loans would relieve some of that financial stress.

The government program could also work with companies such as RMS and AIR, which primarily model catastrophic property events and provide their models to private insurers and reinsurers. This modeling company would develop many scenarios that represent theoretically possible catastrophic cyber attacks and acts of cyber terrorism. For example, a group of scenarios could represent different lengths of time that a region of the country experiences a power blackout resulting from a cyber attack on power grids. The modeling company would then estimate the costs that different classifications of companies would experience based on an identified exposure base for each type of insurance coverage. In this example, the exposure base for business interruption costs could be the total sales of the insured business. The modeling company would group insured companies into homogeneous groups with similar risk profiles and approximate the costs of each scenario for each group. As the modeling company generates more scenarios and obtains more data for loss cost estimation, insurers can use these estimates to more confidently price products covering costs of extreme cyber events.

While the government program does its part, private insurers and reinsurers can work to enhance their own cyber insurance models. Many cyber attacks in the past have produced claims that would fall below the government reinsurance program's threshold, so the private sector would be fully responsible for these losses. The amount of data available to use in pricing cyber products increases with the number of attacks that occur. Experts feel confident that in the future, cyber attacks will mirror those of the recent past because cyber criminals tend to mimic the actions of other cyber criminals and prefer to attack via tried-and-true methods. Most of these more predictable attacks are specific to just one or a few companies, and thus government intervention is unnecessary. Private insurers have sufficient data and loss knowledge to reasonably predict losses and price certain cyber insurance products.

Insurers can incorporate various emerging modeling methods into their cyber insurance models. Since the majority of the uncertainty surrounding cyber attacks deals with very large or catastrophic losses, extreme value analysis can be helpful in pricing cyber products. Since some models already exist for cyber losses of relatively low amounts, separating the extreme losses from the minor or more conventional losses, and modeling each separately, would be prudent. Insurers could also incorporate copulas into their cyber loss distributions. Using copulas to model the total dollar amount of loss, which is a function of the severity of each loss and the number of losses, offers greater marginal distribution flexibility. The losses for each pricing variable can take any empirical form, and thus pricing actuaries can incorporate the most accurate models into their pricing. Copulas also allow the pricing variables to be interdependent, which can be useful for cyber insurance. For a product covering a business's total loss from identity theft, for example, the amount of total loss depends greatly on the number of customers in the insured business. Matrices that represent networks help a business model its correlated risks. A node-link graph can show how insured companies are technologically related and can be converted into a matrix used in models. The matrix would show which insured companies are more at risk of an attack if a business using the same online payroll system, for example, experiences a cyber attack on that system.

Property-casualty insurers offering first- and third-party cyber insurance coverage could require strong risk management practices for businesses to qualify for cyber insurance policies. For example, companies would have to prove their security networks meet certain standards before receiving coverage, just as NFIP requires newly constructed buildings in areas prone to flooding to be elevated to a minimum height. These requirements would force companies to maintain strong risk management practices even though their cyber insurance serves as a security blanket. In addition to requiring these minimum risk management practices for coverage, insurers could charge lower premiums as companies move toward excellent or extraordinary risk management.

This government reinsurance program would allow the private and public sectors to work simultaneously and cooperatively to model cyber risks and provide highly demanded cyber insurance

products to companies. As the threat of large-scale cyber attacks looms in the not-so-distant future, more companies are looking to shift cyber risk to other parties, and insurers and reinsurers are eager to enter a potentially lucrative market. While the private sector and government work out the insurability issues of cyber risk, the government reinsurance program would remain intact to provide needed coverage for large cyber losses. Once the private sector feels confident that it can insure all kinds of cyber risk, the government intervention program would no longer be necessary and could be allowed to expire.

Chapter 6

Conclusion

The world of cyber risk is exciting, dynamic, and expanding. More and more property-casualty insurance and reinsurance companies are entering this relatively new market as the demand for cyber insurance products increases. However, the aspects of cyber risk that make it so interesting and stimulating are also causing the private sector to struggle. Researchers and experts in the cyber field report that there is an increasing probability of the occurrence of cyber attacks causing losses larger than ever before seen. These severe, unpredictable, and perhaps unimaginable attacks cause many in the cyber insurance field to worry. Can the private sector confidently insure against all potential cyber threats, or should the government step in, at least temporarily, to ease the private sector's financial burden?

This question may be debated for decades or centuries to come. The government's role in administering health insurance, which was first offered by the private sector in the mid 1800s, is still the topic of much political and business world debate over a century later. As cyber insurance becomes a more popular focus in the private insurance sector, it may be just a matter of time before the government needs to intervene. Many insurance and reinsurance companies would welcome some type of government intervention because many customers want more sizable coverage than the private insurers and reinsurers feel comfortable offering. Until they feel confident in their pricing mechanisms, most private insurers will not want to insure larger cyber risks. A temporary government reinsurance program could ease the worries of both the insureds and the insurers.

A government insurance program could help private insurers and reinsurers get access to more data about cyber attacks of all sizes. It could ease the financial stress of these companies as well by promising to take financial responsibility for cyber attacks producing claims above a certain threshold. By working with scenario modeling companies, the government could expedite the private sector's attempts

to model all types of cyber risk. Simultaneously, the private sector could develop and define their cyber product offerings and collect historical data to use in their pricing models. They could feel comfortable selling products with higher limits than those currently in place because if a catastrophic cyber attack occurred, they would know they have government backing. This program might also draw high-technology companies to the United States because a cyber reinsurance program like this one does not exist in any other country.

Although people may argue about the exact provisions of a government cyber reinsurance program, many agree that government intervention is needed soon before a cyber attack occurs producing losses like those experienced on 9/11. All kinds of industries are getting interested in purchasing cyber insurance, from financial and retail companies to companies in the manufacturing and education fields. Although cyber risk is considered "new" and "exciting," the goal of this proposed government reinsurance program is to eventually make cyber risk "conventional" and "boring" for insurers. Once the private sector has enough historical data, sound pricing methodologies, and the financial capacity to insure the risk of catastrophic losses from cyber events, the program will have completed its purpose and can cease to exist.

APPENDIX

LAW OF LARGE NUMBERS EXAMPLE

Suppose each person in an identically distributed and independent group faces a loss of $100,000 with probability 0.01 and pays a premium of $4,000, or four times the expected loss of $1,000 per person. Table 5 shows that the number of losses that can be absorbed by the pool and the probability of the pool failing depends on the number of units in the pool.

Table 5. Law of Large Numbers Example

Number of Units in Pool	Number of Losses that can be Absorbed with Pooled Funds	Probability that Pool Will Fail
1	0	.01
2	0	.0199
3	0	.0297
…	…	…
24	0	.2143
25	1	.0258
26	1	.0278
…	…	…
49	1	.0864
50	2	.0138
51	2	.0145
…	…	…
99	3	.0178
100	4	.0034
101	4	.0036
…	…	…
124	4	.0084
125	5	.0017
…	…	…

The pooled funds can only absorb a loss when there are at least twenty-five people in the pool because if a loss occurs, it will equal $100,000. However, each person is only contributing $4,000 to the pool, and if twenty-five people contribute, the insurer will have exactly $100,000 to cover only one loss.

The probability that the pool will fail when only one person is in the pool is 0.01 because the pool will only fail if that one person has a loss, which has a probability of 0.01. When two people are in the pool, the probability of the pool failing equals the probability of at least one of the two people having a loss, because the $8,000 collected in premium would not be sufficient to cover either $100,000 or $200,000 of loss. This probability of 0.0199 is calculated as 2*0.01*0.99 (the probability that only one person has a loss) plus 0.01^2 (the probability that both people have a loss). With three people in the pool, the probability of the pool failing equals 0.0297, or $3*0.01*0.99^2$ (the probability that only one person has a loss) plus $3*0.01^2*0.99$ (the probability that only two people have a loss) plus 0.01^3 (the probability that all three people have a loss). The rest of these probabilities can be calculated in a similar manner.

As shown in the table, when less than twenty-four people buy insurance, adding one more insured person to the pool increases the pool's probability of failure. The additional premium gained still will not help cover even one loss, but since another person joins the pool, the odds of a loss occurring increase. At twenty-five units, the probability of failure falls, but then continues to increase again with the addition of more units. Every twenty-five units, the probability of failure drops to a new low and the pool has the capacity to absorb one more loss. Once the number in the pool equals or exceeds one hundred, the probability of failure is always less than 0.01. Thus the insurer feels more comfortable when there are more people in the insured pool.

The Law of Large Numbers also implies that as the number in the pool increases, the expected value of the loss will stay the same, but the standard deviation (a measure of risk) will decrease. The standard deviation of the loss equals the square root of the variance of the loss. With one person in the pool, the variance equals $0.01*100{,}000^2$ (the expected value of the squared loss) minus $(.01*100{,}000)^2$ (the expected value squared), or 99,000,000. Thus, the standard deviation is approximately 9,950. The standard deviation of the pooled loss equals the unpooled standard deviation of 9,950 divided by the square root of the number of people in the pool. With one hundred units in the pool, the standard deviation reduces to about 995, which correlates to a lot less risk for the insurer. This diminishing

standard deviation is another reason why insurers feel that the risk of losses is more insurable if they have enough independent and homogeneous exposure units to pool together.

This example was recreated from Smith and Kane's "Law of Large Numbers and the Strength of Insurance."[34]

[34] See [26], pp. 8-13.

BIBLIOGRAPHY

1. Baribeau, Annmarie Geddes. "Cyber Insurance: The Actuarial Conundrum." *Actuarial Review* July 2015: 32-38. Print.
2. "Catastrophes: U.S." *Insurance Information Institute*. Insurance Information Institute, 2015. Web. 29 Dec. 2015.
3. Chabinsky, Steven. "Got Cyber Insurance?" *Security* 52.6 (2015): 32. *ProQuest.* Web. 19 Dec. 2015.
4. Coomber, John R.. "Natural and Large Catastrophes — Changing Risk Characteristics and Challenges for the Insurance Industry". *The Geneva Papers on Risk and Insurance. Issues and Practice* 31.1 (2006): 88–95. Web.
5. "Cyber Risks Explained." *National Corporate Practice*. Marsh, 2011. Web. 19 Dec. 2015.
6. "Cybersecurity." *National Association of Insurance Commissioners*. The Center for Insurance Policy and Research, 29 Sept. 2015. Web. 20 Dec. 2015.
7. Feng, Wan. *The Distinctive Characteristics of Life Insurance Operation*. N.p.: China Life, May 2007. PPT.
8. Frean, Alexandra. "JP Morgan Victim of Largest Hack of Customer Data." *The Times* [London] 11 Nov. 2015, Business sec.: 50. Print.
9. Glascott, Michael T., and Aaron J. Aisen. "The Emperor's New Clothes and Cyber Insurance." *FDCC Quarterly* 63.3 (2013): 200-25. *ProQuest.* Web. 19 Dec. 2015.

10. "Google Acts Over China Hack." *Computer Weekly* (2010): 8. *ProQuest.* Web. 22 Dec. 2015.

11. Gray, Dahli, and Jessica Ladig. "The Implementation of EMV Chip Card Technology to Improve Cyber Security Accelerates in the U.S. Following Target Corporation's Data Breach." *International Journal of Business Administration* 6.2 (2015):60, n/a. *ProQuest.* Web. 23 Dec. 2015.

12. Haggard, Stephan, and Jon R. Lindsay. "North Korea and the Sony Hack: Exporting Instability through Cyberspace." *Asia - Pacific Issues*.117 (2015): 1-8. *ProQuest.* Web. 23 Dec. 2015.

13. Harrison, Ann. "Analysts: Mafiaboy Only Amateur Copycat." *Computerworld* 34.17 (2000): 6. *ProQuest.* Web. 22 Dec. 2015.

14. Herath, Hemantha S.B., and Tejaswini C. Herath. "Copula-based Actuarial Model for Pricing Cyber-insurance Policies." *Insurance Markets and Companies: Analyses and Actuarial Computations* 2.1 (2011): 7-20. Print.

15. "High Risk List: National Flood Insurance Program." *U.S. Government Accountability Office*. U.S. Government Accountability Office, 2015. Web. 02 Jan. 2016.

16. Kapoor, Amitesh and Utkarsh Shrivastava. "Extreme Values Theory and Return Level Analysis for Catastrophe Prediction." *Journal of Investing* 23.2 (2014): 124-35. Print.

17. "KID HACKS NASA." *InternetWeek*.853 (2001): PG9. *ProQuest.* Web. 22 Dec. 2015.

18. King, Rawle O. "National Flood Insurance Program: Background, Challenges, and Financial Status." *Congressional Research Service* (2011): 1-29. *Federation of American Scientists*. Congressional Research Service, 11 July 2011. Web. 2 Jan. 2016.

19. Law, Jonathan, ed. "Insurable Risk." *A Dictionary of Finance and Banking*. 5th ed. N.p.: Oxford UP, 2015. Print.

20. Lynch, Jim. "History Likely Not Enough to Price Ever-Shifting Cyberrisk." *Actuarial Review* Nov. 2015: 43. Print.

21. Nordqvist, Christian. "Health Insurance." *Medical News Today*. MediLexicon International Ltd., 21 July 2012. Web. 29 Dec. 2015.

22. Oltsik, Jon. "The State of Cyber Insurance." *Network World (Online)* (2015)*ProQuest.* Web. 19 Dec. 2015.

23. Park, Jin. *Topic 7: Characteristics of an Insurable Risk*. N.p.: Illinois Wesleyan University, n.d. PPT.

24. *Property-Casualty Insurance Basics*. Washington, D.C.: American Insurance Association, n.d. PDF.

25. Schmit, Joan T. "A New View of the Requisites of Insurability." *The Journal of Risk and Insurance* 53.2 (1986): 320-29. Print.

26. Smith, Michael L., and Stephen A. Kane. "The Law of Large Numbers and the Strength of Insurance." *Insurance, Risk Management, and Public Policy*. Ed. S. G. Gustavson. N.p.: Kluwer Academic, 1994. 1-27. Print.

27. Solnik, Claude. "Cyber Insurance Policies all the Rage." *Long Island Business News* (2014) *ProQuest.* Web. 19 Dec. 2015.

28. "The History of Cyber Attacks - A Timeline." *NATO Review*. NATO, 2013. Web. 22 Dec. 2015.

29. Thompson, Jon. "The Morris Worm." *Personal Computer World* (2009)*ProQuest.* Web. 22 Dec. 2015.

30. “Trefis: EBay Suffers Hack Attack.” Chatham: Newstex, 2014. *ProQuest.* Web. 23 Dec. 2015.

31. Vijayan, Jaikumar. "5 THINGS YOU SHOULD KNOW ABOUT CYBER INSURANCE." *Computerworld Digital Magazine* 1.11 (2015): 27-32. *ProQuest.* Web. 19 Dec. 2015.

32. Webel, Baird. "The Terrorism Risk Insurance Act of 2002: A Summary of Provisions." *CRS Report for Congress* (2004): 1-6. *CRS Report for Congress*. CRS, 28 Apr. 2004. Web. 3 Jan. 2016.

33. Willis, Henry H., and Omar Al-Shahery. "National Security Perspectives on Terrorism Risk Insurance in the United States." *RAND Reports* (2014): 1-21. *RAND*. RAND Corporation, 2014. Web. 3 Jan. 2016.

34. Wong, Pak Chung, Patrick Mackey, Harlan Foote, and Richard May. "Visual Matrix Clustering of Social Networks." Ed. Mike Potel. *Applications* (2013): 88-96. *IEEE Xplore Digital Library*. Web. 30 Dec. 2015.

35. Zahra, El Arif Fatima. "Introduction to the Extreme Value Theory Applied to Operational Risk." *International Journal of Innovation and Applied Studies* 3.1 (2013): 249-54. Print.

ACADEMIC VITA

Academic Vita of Colleen Tygh
colleentygh@gmail.com

EDUCATION

The Pennsylvania State University (University Park, PA) — Class of May 2016

Schreyer Honors College, Smeal College of Business
Bachelor of Science: *Risk Management – Actuarial Science Option* — Dean's List (all semesters)
Minors: *Economics, International Business, Statistics* — Evan Pugh Scholar

Hochschule Pforzheim University (Pforzheim, Germany) — May – June 2013
Summer Study Abroad Program for International Business and German Language

ACTUARIAL EXAMINATIONS/VEES

SOA Probability/CAS 1—Passed — January 2014
SOA Financial Mathematics/CAS 2—Passed — August 2014
SOA Models for Financial Economics/CAS 3F—Passed — July 2015
Major coursework will satisfy all VEE requirements — May 2016

WORK EXPERIENCE

XL Catlin (Exton, PA) — May – August 2015
Actuarial Intern for Pricing Department's Models & Metrics Team

- Developed VBA and Microsoft Excel skills through many small projects involving insurance pricing models
- Analyzed increased limit factors used in the umbrella model that resulted in substantial changes to the model
- Presented the results of my projects to underwriters and convinced them to accept the proposed model changes

Voya Financial (West Chester, PA) — May – August 2014
Actuarial Intern for Closed Block Variable Annuities Department

- Used SQL to build inputs for liability models, set up model runs, and sent run requests to IT to produce metrics
- Performed month-end trend summary analyses and updated assumption files with third quarter changes
- Improved efficiency of an input file-building process and presented my methodology to my superiors

LEADERSHIP/ACTIVITIES

Pink Zone (University Park, PA) — August 2012 – Present
President — May 2014 – May 2015
Mailings Director — May 2013 – May 2014

Penn State IFC/Panhellenic Dance Marathon (THON) (University Park, PA) — October 2012 – Present
Donor & Alumni Relations Alumni Engagement Captain — September 2015 – Present
Donor & Alumni Relations Committee Member — October 2014 – February 2015

Sapphire Leadership Program (University Park, PA) — August 2012 – Present
Community Involvement Captain — January 2014 – January 2015
Community Involvement Chair — January 2013 – January 2014