Cyber Insurance: A Thematic Exploration of the Market Knowledge Gaps Insights Into Corporate Decision-Making and Adverse Selection

Research · May 2021

DOI: 10.13140/RG.2.2.23429.42721

1 author:

Henry Szklanny
University of Illinois Urbana-Champaign
1 PUBLICATION **0** CITATIONS

Cyber Insurance: A Thematic Exploration of the Market Knowledge Gaps

Insights Into Corporate Decision-Making and Adverse Selection

8W338492

AP Research

May 12, 2021

Word Count: 5,471

Abstract

The increase in cybercrime is leaving many businesses vulnerable to cyber risks. Although the cyber insurance market is burgeoning with great promise, purchasing insurance indiscriminately is a risk. To that end, this inquiry explored how the corporate decision-making process can be better conducted and understood to help the buyer purchase a policy. This inquiry also explored how adverse selection can be alleviated to make the issuance of a policy easier for the insurer. A case study of a major insurance brokerage firm was used to collect input on a series of questions aimed at gaining insight into these market knowledge gaps. To complement the case study, document analysis supplemented the questionnaire. Respondents from this firm included account executives amongst other professionals. Respondents seem to agree that the decision-making process can be better conducted and understood if companies ① enlist the help of third-party consultants, ② augment their cyber risk awareness, education, and communication efforts, and ③ improve their understanding of their needs and risks. Should adverse selection be alleviated, respondents seem to agree that insurers ought to be straightforward, reputable, and trustworthy with potential buyers. Future research should continue to conduct further inquiry into decision-making by surveying current policyholders to see if new themes emerge.

Keywords: adverse selection, cyber insurance, cyber risk, decision-making process, market

Review of Literature

Introduction

Dependence on the internet has enabled businesses to easily network their assets by storing information online. As business processes become automated, these assets are utilized more intensely (Bandyopadhyay, 2012, p. 23). Consequently, the risks associated with operating online have become a rampant problem concerning many businesses. A 2011 Ponemon Institute study surveyed 583 IT security practitioners in the United States. Their results indicate that 90% of organizations in the study have experienced at least one breach in the past 12 months (Ponemon Institute, 2011). There is no sign of cyberattacks declining anytime soon. For example, a study by Seh et al. (2020) drew inferences from a time series analysis of healthcare data breaches. Their results indicate that breaches such as hacking and IT incidents have increased 73.4% in 2019 from 2018 (Seh et al., 2020, Discussion section). This finding is not surprising because it can hardly be limited to just the healthcare industry.

Conventional self-protective measures such as firewalls and antivirus software can help mitigate risk to an extent. However, the means of attack are only limited to the imaginations of the attackers (French, 2018, p. 607). Sources within the cyber insurance literature seem to agree since many claim that protection through technical means alone is suboptimal (Bandyopadhyay et al., 2009; Bolot & Lelarge, 2009; Pal et al. 2014; Shields, 2019). As a result, businesses are forced to operate with residual cyber risk.

Realizing that it is essentially impossible to eliminate all residual cyber risk through technical means alone, proponents have suggested investing in cyber insurance. This type of insurance is designed to mitigate losses from a variety of cyber incidents, including business interruption and network damage (Cybersecurity and Infrastructure Security Agency [CISA], n.d.). The insurance company agrees to bear losses incurred by cyber incidents and in return receives a recurring policy premium from the policyholder (Toregas & Zahn, 2014, Dealing With Cyber Attacks section, para. 4).

The cyber insurance market is hectic, and the anticipation of an attack can make it tempting to purchase insurance indiscriminately. Individual experience and media coverage of cyberattacks can also play a role in shaping risk perception (De Smidt & Botzen, 2018, p. 240). De Smidt and Botzen (2018) used a survey research method to gauge the responses of 1,891 professional decision makers on risk perception variables. They found that "of respondents who estimate a high financial impact …, 71.4 percent have a high degree of worry … as opposed to 32.5 percent who are worried … and 27.3 percent who are indifferent" (p. 253). While purchasing cyber insurance is worth considering, spending out of fear is a risk. There is a need for more research on how the decision-making process can be improved because according to Lloyd Foster, an adjunct actuarial instructor at Columbia University, in this "rush to fill a gap, the decision makers are going ahead without sufficient actuarial involvement" (Baribeau, 2015, p. 35). According to Stephens (2020), insight into this area "will help businesses to better allocate budget appropriately, as they will know what risk their cyber security spend will mitigate,

how much cyber insurance they need to buy and what residual amount is within their appetite to retain" (p. 14).

The remainder of this literature review is organized as follows. Section I sets the context by discussing the current situation of the cyber insurance market. Section II discusses risk transfer and the confusion surrounding cyber risk exposure. Section III discusses the difficulty in pricing premiums. The discussions in sections II and III serve as the prelude to research gap ①, that is, determining how the decision-making process can be better conducted and understood. Section IV discusses adverse selection, and it serves as the prelude to research gap ②, that is, determining how companies can be made more willing to release security information to insurers. The Conclusion and Gaps section will discuss the importance of addressing these gaps.

I Current Market Situation

The market has gained significant traction since its inception in the late 1990s. Whereas most companies did not have cyber insurance even just a decade ago, one in three now has insurance specifically for cyber risk coverage (Fernandes, 2014, para. 2). Larger companies used to be the chief buyers of cyber insurance, and smaller companies were less likely to purchase coverage. That, too, seems to be changing (Betterley, 2010; Advisen, 2013). These observations would initially suggest that the market is growing, but others contend that it is moving at a sluggish pace. Cylinder (2008) conducted an evaluation of the market and points out that there are "major obstacles preventing development into a full-fledged industry" (p. 15). In a similar evaluation, Marotta et al. (2015) concluded, "despite a slow start and many problematic issues, the market grows" (p. 40). This ultimately raises two questions—what are the specific issues, and how can they be solved?

II Risk Transfer

Should conventional security solutions fail, cyber insurance allows a company to transfer their cyber risk. Many companies are, however, struggling to understand their cyber risk exposure, and this lack of understanding creates an impediment for every company that could benefit from risk transfer. Decision-making is what Marotta et al. (2015) refer to as 'Phase 0: Self-Assessment and Treatment by an Agent' of the insurance process. In this phase, "an agent performs self-assessment and decides which risk it would like to transfer and whether the transfer option is more efficient rather than others" (Marotta et al., 2015, p. 12). Risk transfer can be a favorable way of handling residual cyber risk. But given the lack of understanding of self-assessment, it is unsurprising when skeptics conclude that "it is hard to specify what an insured wants to be covered from" (Carfora et al., 2018, p. 202). It would also come as unsurprising when companies forego policies citing confusion about what they cover and uncertainty that their organizations will suffer a cyberattack (CISA, n.d.). Companies must be able to know how to conduct a self-assessment of their cyber risk exposure. There is limited research on how the decision-making process can be improved. Addressing this gap could potentially give companies a better understanding of what risks they face and how to better conduct a self-assessment.

III Pricing Premiums

Pricing premiums has traditionally relied on actuarial tables constructed from historical records (Gordon et al., 2003, p. 82). Unlike traditional insurance products, historical records on cybercrimes are scarce (Eling, 2020, p. 327) because the internet is relatively new, and information is mostly proprietary. Due to a limited ability to quantify cyber costs, insurance companies are pricing policies conservatively, that is, at a higher price (Toregas & Zahn, 2014, The Issue of Setting Premiums in Context section, para. 5). This is problematic for potential buyers, and so it is unsurprising when conservative pricing of premiums is often cited as the primary reason for limited growth of the market (Bandyopadhyay et al., 2009, p. 68). The market is competitive, and insurers are more focused on building market share than ensuring accurate premiums. This challenge once again calls into question the decision-making process. Cyber insurance is worth considering, but companies ought to know how much they are willing to reasonably invest. Insight into this area "will help businesses to better allocate budget appropriately, … how much cyber insurance they need to buy and what residual amount is within their appetite to retain" (Stephens, 2020, p. 14). Furthermore, "such research is helpful, as it empowers … companies to realize that they might be paying too much for their policies" (Toregas & Zahn, 2014, The Issue of Setting Premiums in Context section, para. 8).

IV Adverse Selection

Whilst the insured may suffer from the possibility of overpaying for premiums, a lack of data also has negative effects on the insurer. Whereas phase zero was concerned with the buyer, phase one of the insurance process is concerned with the insurer— 'Issue Insurance Policy to an Agent' (Marotta et al., 2015, p. 12). When an agent decides to buy an insurance policy, the insurer needs to estimate the risk of the agent, a step called "impact determination" (Marotta et al., 2015, p. 12). To do this, the insurer would typically conduct interviews, distribute questionnaires, or use a knowledge base (Marotta et al., 2015, p. 27). It is here where frustrations arise because adverse selection is "the problem that arises because a firm (or person) choosing to insure against a particular loss is likely to have private information not available to the insurance company at the time of contracting" (Gordon et al., 2003, p. 82). This frustration is what Marotta et al. (2015) refer to as an "information sharing barrier" (Marotta et al., 2015, p. 20). While adverse selection is not unique to the cyber insurance market, the difficulty in pricing premiums "is further exacerbated by the reluctance of organizations to reveal details of security breaches" (Herath & Herath, 2011, p. 9). Other lines of insurance have dealt with this challenge for years and have gathered enough experience to alleviate it. The cyber insurance market is still in a nascent stage, and so adverse selection is still a challenge. Some insurers are, however, using sophisticated technology and other tools to overcome this barrier (Toregas & Zahn, 2014, Evolution of the Market and Challenges section, para. 4).

How have other lines of insurance been able to overcome this barrier? For one, health and life insurance underwriters may require physical examination records. They may then discriminate between individuals based on lifestyle choices such as smoking versus nonsmoking. In the cyber insurance market, adverse selection comes down to the likelihood of a security breach. Cyber insurers can discriminate against those who do not invest in self-protective measures. However, this may not be enough information to sufficiently differentiate between high and low risk individuals. Some companies are unwilling to disclose information about their cyber incidents. To deal with uncertainty in pricing, insurers may require security audits, which is the equivalent of the student transcript required to obtain reduced teen driver premiums, for example. And so, the problem is clear—if buyers are unwilling to release information, the insurers may not be able to differentiate between high and low risk individuals, leading to inaccurate premiums. “If premiums are priced too high then other insurers will reap the windfalls. However, if an insurance firm is inaccurate in quantifying the cyber-risks in premiums that are priced too low, then large losses may result” (Majuca et al., 2006, p. 2). Little research has been done on what insurers can do to increase company willingness. Such information would be valuable in alleviating adverse selection.

Conclusion and Gaps

Cyber insurance is the fastest growing product the insurance industry has ever seen. A popular argument made in its favor is its ability to absorb losses incurred by cyber incidents. Should conventional security solutions fail, cyber insurance allows a company to transfer their cyber risk. In addition, customization allows the insurer to tailor a policy to meet the needs of the company, making it an appealing risk transfer option. Despite hopeful prospects, the literature maintains that the market is still nascent, and therefore has unique challenges that prevent it from maturing. These challenges include, but are not limited to, a lack of understanding of the decision-making processes and adverse selection. The motivation for including both topics is that of the many issues facing the market, addressing these topics is paramount to its future success and maturity into a full-fledged industry. These two topics and their accompanying questions are fundamental in every line of insurance, and this market's inability to overcome the most basic challenges impels us to look at them closely.

This paper will attempt to add insight into two gaps—gap ①, that is, determining how the decision-making process can be better conducted and understood and gap ②, that is, determining how companies can be made more willing to release security information to insurers. I believe that addressing gap ① will help companies during the decision-making process and perhaps alleviate the confusion in assessing individual risk. Many insurers are using sophisticated technology to overcome adverse selection, but nobody seems to be asking the obvious question namely how companies can be made more

willing to release information. I believe that addressing gap ② will help insurers alleviate adverse selection during information sharing. This culminates into the research questions this paper will attempt to answer—How can the decision-making process be better conducted and understood to help the buyer purchase a policy, and how can adverse selection be alleviated to make the issuance of a policy easier for insurer? I believe that addressing these questions and gaps will contribute to increased development of the cyber insurance market.

Methodology

Justification of Methods

To address these gaps, I followed the advice of Tøndel et al. (2015), who recommend using a case study design as the primary research method combined with another relevant method when conducting qualitative research on cyber insurance knowledge gaps. I conducted a case study of a major insurance brokerage firm[1] in which an online questionnaire was used to gauge and collect responses. I also conducted document analysis to complement the case study. This triangulated research design has increased the quality and validity of the study. Such is the belief because the goal is to present new findings surrounding the decision-making process and adverse selection—gaps that are relatively new and therefore not fully understood. A case study of this firm has allowed me to understand how this firm consults their clients during decision-making,

[1] This firm will be referred to as 'Firm X' for the remainder of this paper

which has been helpful in generating new ideas about this gap. Document analysis has worked particularly well as a complement because it has supplemented for limited or basic responses.

Construction of Methods

In constructing the questionnaire for the case study, I used 14 questions not including those regarding demographic and background information. Of these, three were generated by me (self-generated)[2]. The remaining 11 were adapted from or influenced by previous studies and papers. Of those 11 questions, five were adapted from Tøndel et al. (2015)[3], who recommend studying the selected questions in their recommendations for further research on cyber insurance knowledge gaps. Three questions were also adapted from a questionnaire used by Toregas and Zahn (2014)[4]. Two statements from Shukla (2018)[5] were adapted into likert statements. And finally, another statement from Carfora et al. (2018)[6] was adapted into a question. These questions and statements were used because they were all deemed pertinent in providing meaningful insight into the research gaps. For example, Tøndel et al. (2015) provide a list of cyber insurance knowledge gaps and a list of specific questions for addressing each gap. In choosing the questions, I combed through the list of recommendations to select those most pertinent to the purpose of my

[2] Denoted SG in the Appendix
[3] Denoted α in the Appendix
[4] Denoted β in the Appendix
[5] Denoted γ in the Appendix
[6] Denoted δ in the Appendix

inquiry.

The questionnaire was created and administered using Google Forms. The questionnaire was organized into four sections: informed consent, demographics, background, and questions. Respondents were required to read and agree to the consent notice before proceeding. The demographic section collected information such as age, gender, and ethnicity. The background section collected information such as years of experience, job title, and company location. The questions section was the main section of the questionnaire. Here, the questionnaire consisted of questions aimed at gaining insight into the gaps. Personally identifiable information was never collected. The questionnaire was open for approximately 14 days. Below are just a few of the questions and question styles used in the questions section[7]. The questions in Figure I were aimed at gaining insight into the first research question, that is, gap ①. The questions in Figure II were aimed at gaining insight into the second research question, that is, gap ②.

[7] The full questionnaire can be found in the Appendix

Figure I

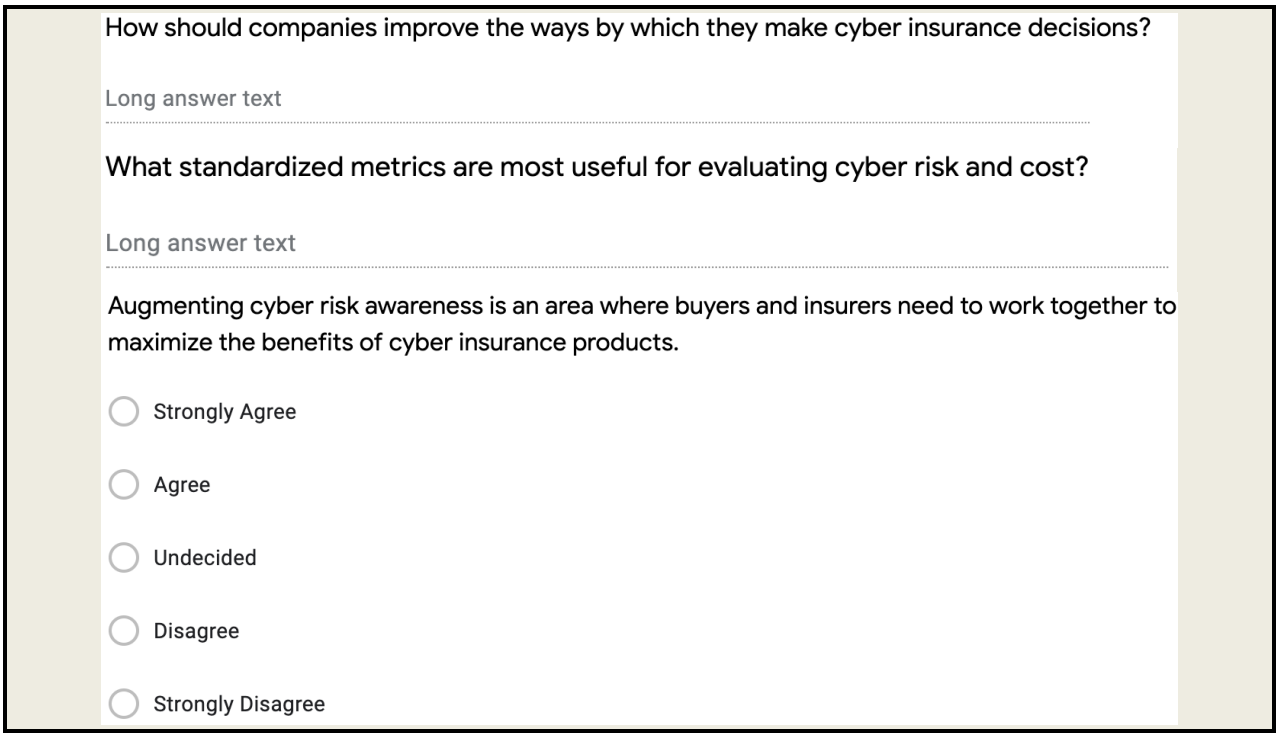
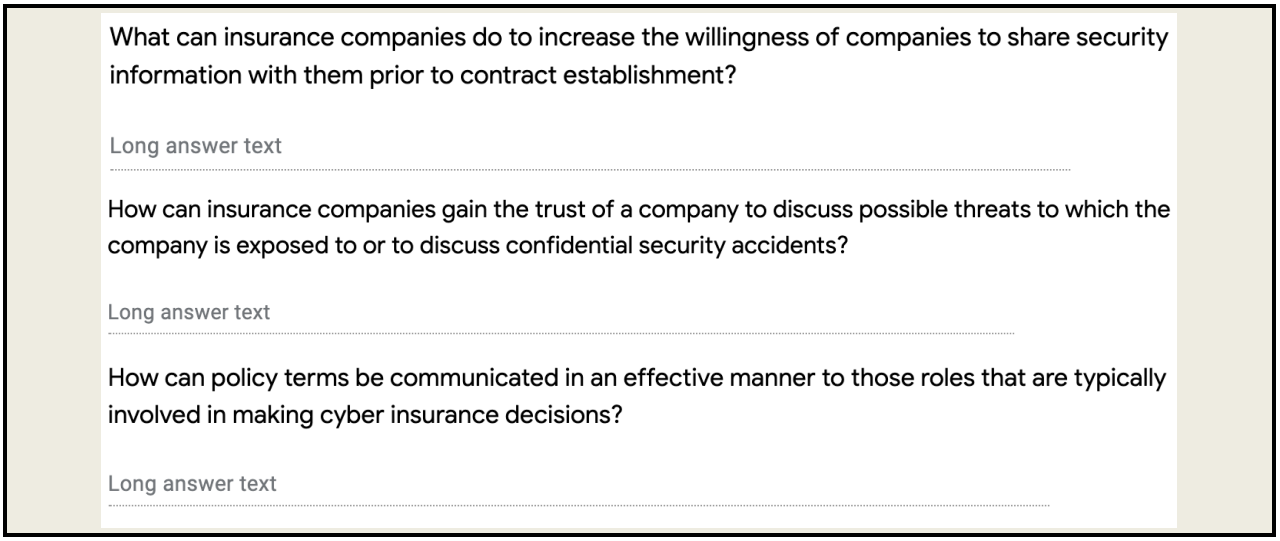


Figure II



In preparing for document analysis, four online documents were provided to me by a participant who is employed by Firm X. Only two of the four documents were analyzed because the other two discuss cyber insurance market updates and trends—information that is not necessary for this inquiry. The analysis of the two selected documents has provided a deeper understanding of gap ① because one of the documents[8] shares details about the ins and outs of the Governance Process used by Firm X during consultation. The second of these documents[9] is a playbook that contains excellent information about exposure quantification and understanding corporate cyber risk. This document also discusses Firm X's Three-Step Approach to understanding corporate cyber risk.

[8] This document will be referred to as 'document Ⓐ' for the remainder of this paper

[9] This document will be referred to as 'document Ⓑ' for the remainder of this paper

Participants

The questionnaire was distributed to approximately 25 people, of which only eight participated. One participant was recruited by me, and the remaining six were recruited through a personal connection of mine. My personal connection also partook in the completing questionnaire. Most of the respondents (six) are employed by Firm X. The remaining two participants are not employed by Firm X, but I still deemed them appropriate for completing the questionnaire given their knowledge and experience. Those participants who are not employed by Firm X were not included in the case study. I believe that the case study of Firm X has produced meaningful insight into how the account executives consult their clients during decision-making. And I believe that this audience has provided meaningful insight given their relevant experience in fields such as insurance, insurance broking, and risk management.

Protocol for Analysis of the Case Study

I found multiple themes whilst analyzing the responses. “Themes” should be understood as the major findings based on the agreement of thought amongst respondents. I thematically analyzed the responses from the questionnaire—a process known as coding. The commonalities uncovered from this analysis were then organized into major themes which were then contextualized to draw conclusions. The purpose of the case study of Firm X was to gain a deeper understanding of how this firm consults their clients during decision-making. However, two participants who are not employed by Firm X were given permission to complete the questionnaire anyway. To make the case study fully representative of Firm X, a distinction is made in-text between those employed by Firm X and those who are not when discussing themes. This distinction is also facilitated using tables.

Findings and Analysis

Demographics and Background

Twenty-five percent of participants are in the 18-24 age group, 62.5% are in the 25-34 age group, and one respondent comprising 12.5% of the total is in the 35-44 age group. Responses were received from metropolitan areas across the United States including Los Angeles, Chicago, and New York City. Eighty-seven-point five percent of the respondents have said that their profession is in the insurance field, and of these, the average years of experience in this field is approximately eight years. Some of the participants include an actuarial specialist, a vice president account executive, and an account executive for cyber technology practice.

Findings of the Case Study

I Third Party Consulting

The first theme I found is the suggestion of enlisting the help of third-party consultants. Many respondents encourage finding a good broker or enlisting third party consultants when considering cyber insurance. For example, Respondent Ⓐ said, “To help assess their cyber risk, they can speak to trustworthy cyber risk consultants to understand what is at stake and what actions should be taken.” Respondent © seems to agree in saying that “if buyers are confused or unsure, find a good broker and an easy-to-understand cyber program.” Respondent Ⓑ also mentions the confusion surrounding cyber risk exposure and self-assessment and said that “leveraging/partnering with specialized third-party firms at multiple points when navigating the confusion is typically very helpful.” Four of the six respondents employed by Firm X specifically mentioned the use of third-party consultants or insurance brokers in their response, and one of the two respondents not employed by Firm X speaks similarly. Table I organizes the responses of this theme.

Table I

Respondent	Respondent employed by Firm X?	Respondent's job title/profession	In response to question number	Response
Ⓐ	No	Actuarial Specialist	15	"And to help assess their cyber risk, they can speak to trustworthy cyber risk consultants to understand what is at stake and what actions should be taken."
Ⓐ	No	Actuarial Specialist	23	"Since cyber attacks/incidents are fairly new in the actuarial realm, third parties should highly be considered for consulting."
Ⓑ	Yes	Account Executive, Cyber Technology Practice	12	"It is on insurance brokers to advise and consult with clients on exposures and the cyber threat environment."
Ⓑ	Yes	Account Executive, Cyber Technology Practice	15	"Leveraging/partnering with specialized third party firms at multiple points when navigating the confusion is typically very helpful."
Ⓑ	Yes	Account Executive, Cyber Technology Practice	22	"specialized insurance brokers"
Ⓒ	Yes	VP	17	"If buyers are confused or unsure, find a good broker and an easy to understand cyber program."
Ⓔ	Yes	VP, Head of Major Accounts	22	"with a good broker"
Ⓖ	Yes	Senior Financial Analyst	13	"I imagine having a broker would help a company make cyber insurance decisions by outsourcing that decision making process to the broker that specializes in the topic."
Ⓖ	Yes	Senior Financial Analyst	15	"Depends on the company - some companies could probably do this internally, but I imagine most would be better off using a third party (I.e. consultant/broker) to help them navigate and assess their situation."

II Augmenting Awareness, Education, and Communication

Another theme that emerged in the thematic analysis is the notion of augmenting awareness, education, and communication efforts. Respondents seem to agree that augmenting these factors amongst decision-makers and employees is important before and during decision-making. For example, Respondent Ⓑ said, “Rarely have I seen an organization fully understand their cyber exposure until after they experience an event (ransomware, data exfiltration, etc.). Awareness and willingness to address cyber risk is increasing, but the increase is not fast enough to keep up with the threat environment that companies face.” Awareness can be increased through, according to Respondent Ⓐ, “education and resources that discuss cyber risk and how it can be mitigated.” I found that all (100%) respondents either strongly agree or agree with the statement: “Augmenting cyber risk awareness is an area where buyers and insurers need to work together to maximize the benefits of cyber insurance products.” This data is shown in Figure III. Five of the six respondents employed by Firm X specifically mentioned augmenting either awareness, education, or communication, and both respondents not employed by Firm X speak similarly. Table II organizes the responses of this theme.

Figure III

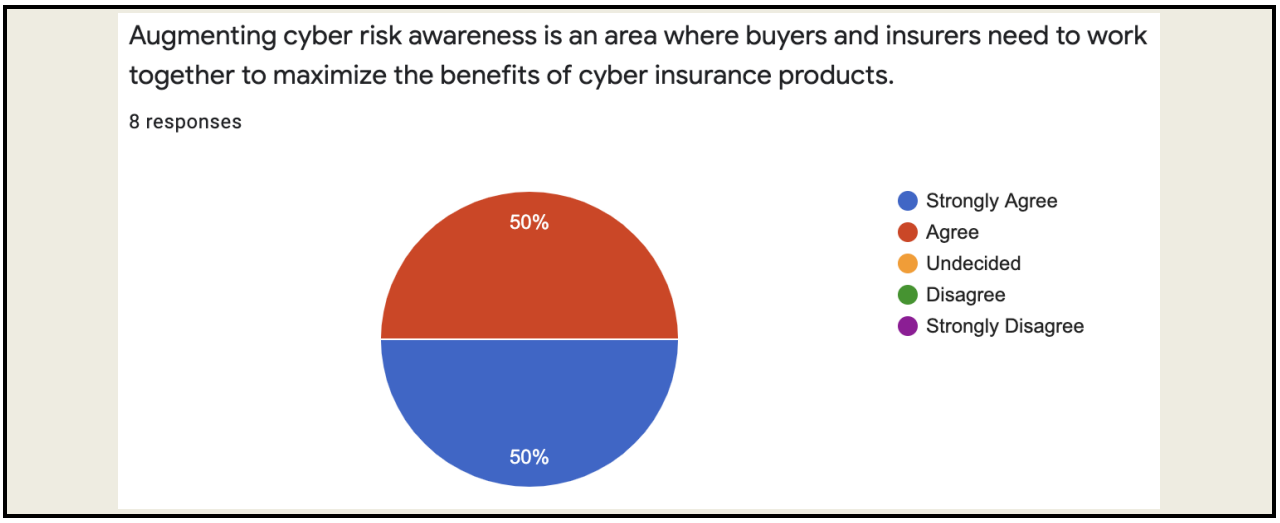

Augmenting cyber risk awareness is an area where buyers and insurers need to work together to maximize the benefits of cyber insurance products.
8 responses
50%
50%
Strongly Agree
Agree
Undecided
Disagree
Strongly Disagree

Table II

Respondent	Respondent employed by Firm X?	Respondent's job title/profession	In response to question number	Response
Ⓐ	No	Actuarial Specialist	13	"They should consider the risks of cyber security and what would happen if there is cyber insurance vs. if there isn't. Education and information is also key to help make cyber security decisions!"
Ⓐ	No	Actuarial Specialist	21	"education and resources that discuss cyber risk and how it can be mitigated" "Trainings and seminars could be very helpful."
Ⓑ	Yes	Account Executive, Cyber Technology Practice	21	"Rarely have I seen an organization fully understand their cyber exposure until after they experience an event (ransomware, data exfiltration, etc.). Awareness and willingness to address cyber risk is increasing, but the increase is not fast enough to keep up with the threat environment that companies face."
Ⓒ	Yes	VP	21	"Provide employee training on phishing emails and what to do/not to do, etc."
Ⓔ	Yes	VP, Head of Major Accounts	21	"training and testing"
Ⓕ	Yes	Vice President Account Executive	21	"enterprise awareness"
Ⓖ	Yes	Senior Financial Analyst	21	"Like most things, the best answer is a simple one: cyber risk awareness can be increased through communication and education efforts."
Ⓗ	No	Team Lead, Business Intelligence	21	"Communication—but not over-communication—is key to this. In my experience, when a workplace sends many follow ups and incessant reminders about something, it turns many employees off to the idea of actually listening to what the workplace has to say. This is especially true if the topic doesn't directly affect an employee."

III Understanding Needs and Risks of the Company

The final theme I found regarding the decision-making process is the necessity of understanding the needs and risks of the company. Respondents argue that it is imperative to understand and consider the specific needs and risk profile of the company during decision-making. For example, Respondent Ⓐ suggests that “individuals need to evaluate their own risks, and companies should look into whether or not this is in the best interest of their assets and customers.” Others suggest the same. According to Respondent Ⓕ, “They need to evaluate their particular risk as it differs from their peers.” Five of the six respondents employed by Firm X specifically mention understanding the needs and risks of the company, and one of the two respondents not employed by Firm X speaks similarly. Table III organizes the responses of this theme.

Table III

Respondent	Respondent employed by Firm X?	Respondent's job title/profession	In response to question number	Response
Ⓐ	No	Actuarial Specialist	14	"Look at the needs of your company, see if getting cyber insurance aligns with your values and customer protection. Companies should do what is best for them and their customers, and in most situations, protection of confidential information is key, and could be worth investing into."
Ⓐ	No	Actuarial Specialist	17	"Individuals need to evaluate their own risks, and companies should look into whether or not this is in the best interest of their assets and customers."
Ⓑ	Yes	Account Executive, Cyber Technology Practice	17	"By taking an enterprise risk management approach to their cyber exposure.
Ⓒ	Yes	VP	14	"Decide which risks … [and] amounts their business is comfortable self-insuring and which risks and amounts they want to transfer to an insurance company."
Ⓓ	Yes	EVP	14	"appetite of risk and risk profile"
Ⓔ	Yes	VP, Head of Major Accounts	17	"understand their risk and what their current policies cover or exclude as [it] relates to cyber risk"
Ⓕ	Yes	Vice President Account Executive	17	"They need to evaluate their particular risk as it differs from their peers."

IV Straightforwardness, Reputability, and Trust

The only theme I found about the information-sharing barrier and adverse selection is the suggestion that insurance companies be straightforward, reputable, and trustworthy. Some respondents agree that should the information-sharing barrier be alleviated, it is essential that insurers be straightforward, reputable, and trustworthy. For example, Respondent Ⓐ insists that, “Conversations need to be had 100% - without a discussion then there won't be trust. The insurance company providing the cyber insurance needs to be blunt and truthful about their track record in order to gain the trust of companies to obtain their product.” Respondent Ⓒ seems to agree in saying that, “The easiest policy terms to understand are the ones that are written to be straightforward, logical, and organized. If you are trying to communicate effectively with decision-makers, you have to focus on what is most important to them: price, ROI, and reputation (both internal and external) are among the highest values.” Three of the six respondents employed by Firm X explicitly mention that insurers ought to be straightforward, reputable, and trustworthy, and both two respondents not employed by Firm X speak similarly. Table IV organizes the responses of this theme.

Table IV

Respondent	Respondent employed by Firm X	In response to question number	Response
Ⓐ	No	11	"Insurance companies need to be reputable and have a good backing to their promises - I understand that this is difficult for new companies to do, but that's when you can partner with 3rd parties to begin with. Reputability and kept promises are key."
Ⓐ	No	12	"Conversations need to be had 100% - without a discussion then there won't be trust. The insurance company providing the cyber insurance needs to be blunt and truthful about their track record in order to gain the trust of companies to obtain their product."
Ⓐ	No	22	"Highlight the key points, and don't have loopholes embedded - be direct and clear to the potential policyholder."
Ⓒ	Yes	12	"Create simple questions, simple low cost/no cost action items, and provide a simple to understand guide for how businesses implement the needed action items."
Ⓒ	Yes	11	"Figure out a minimal amount of questions that are directly related to preventing cyber claims."
Ⓓ	Yes	22	"Coverage needs to be streamlined."
Ⓖ	Yes	22	"The easiest policy terms to understand are the ones that are written to be straightforward, logical, and organized. If you are trying to communicate effectively with decision-makers, you have to focus on what is most important to them: price, ROI [return on investment], and reputation (both internal and external) are among the highest values."
Ⓗ	No	11	"Contracts are always established in order to share data between companies. However, insurance companies can increase other companies' willingness to share security detail prior to the sale of a cyber risk policy by doing the following:

			- Promising to keep all security detail confidential - Standardizing where security detail is kept. For example, all data on this topic should be stored in a secure folder with an exact list of who has access from both the insurance and the third party company. Access to the folder where this information is stored should be denied unless the person is directly involved with the sale or processing of the policy. - Insurance companies should promise that zero security details will be stored 'in the cloud'. Exposing any data to Microsoft, Google, or other file hosting companies increases exposure exponentially. - Exporting and sending the security detail information to anyone in the insurance company for any purpose should be prohibited unless approved in writing by the 'other' company involved. - The insurance company should promise to keep the list of people with access to this information as short as possible.”
Ⓗ	No	12	“Insurance companies should be willing and able to use hard data (specific numbers, specific positive effects the insurance company has had for others) to show that their guidance has saved other companies from potential ruin.”
Ⓗ	No	22	“Policy terms should be as short as possible while being clear and all-encompassing. Any items that would void coverage or just not be covered should be emphasized as clearly as possible.”

Findings of the Document Analysis

I Governance Process

In analyzing document Ⓐ, I found that Firm X has built their Governance Process around four elements. These elements are summarized in Figure IV.

Figure IV

II Three-Step Approach

In analyzing document Ⓑ, I found that understanding corporate cyber risk can be accomplished through Firm X's Three-Step Approach. These steps are summarized in Figure V and in Figure VI.

Figure V

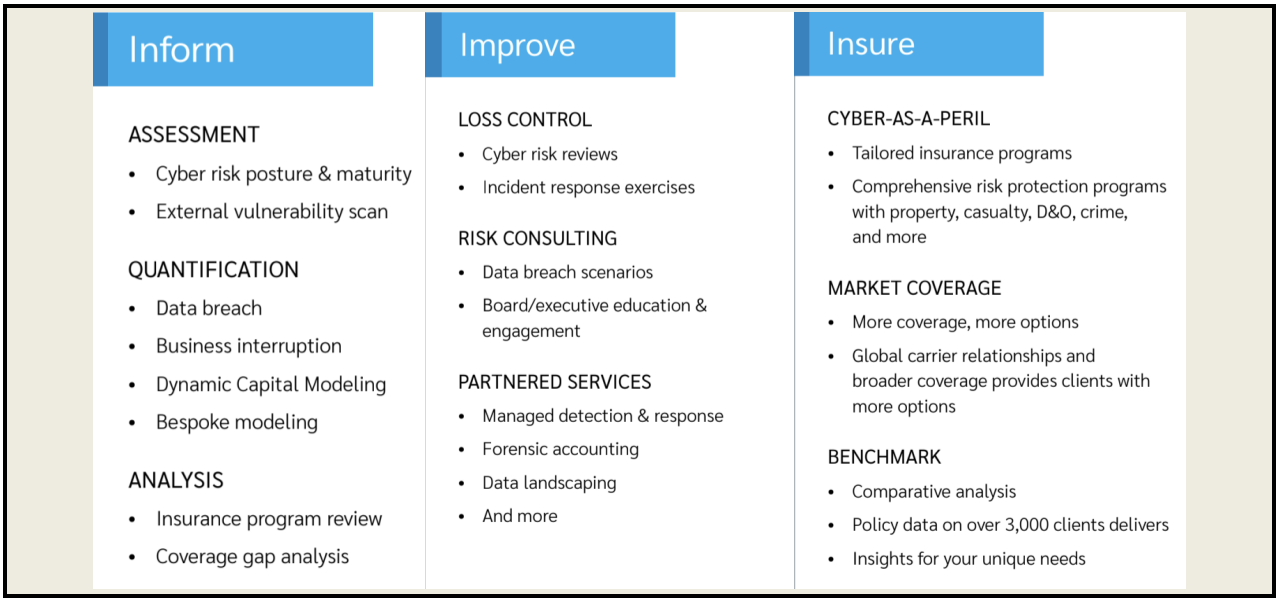
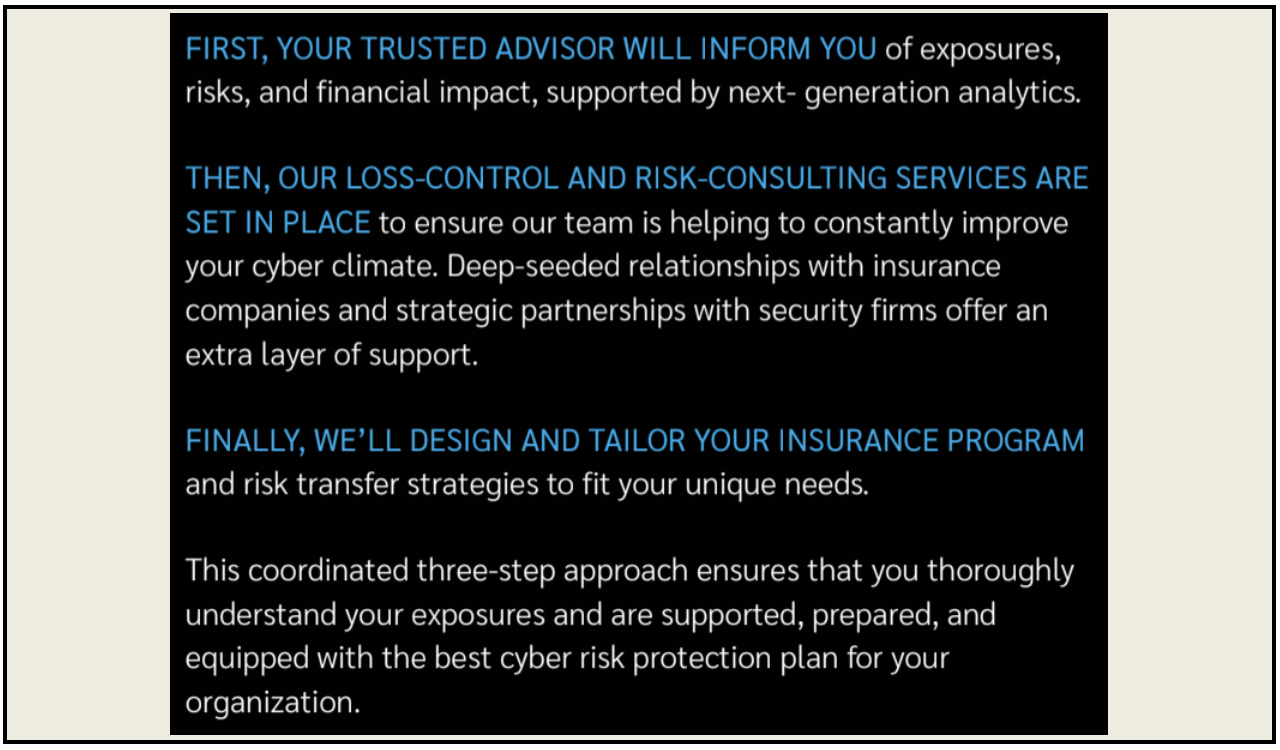


Figure VI


FIRST, YOUR TRUSTED ADVISOR WILL INFORM YOU of exposures, risks, and financial impact, supported by next- generation analytics.
THEN, OUR LOSS-CONTROL AND RISK-CONSULTING SERVICES ARE SET IN PLACE to ensure our team is helping to constantly improve your cyber climate. Deep-seeded relationships with insurance companies and strategic partnerships with security firms offer an extra layer of support.
FINALLY, WE'LL DESIGN AND TAILOR YOUR INSURANCE PROGRAM and risk transfer strategies to fit your unique needs.
This coordinated three-step approach ensures that you thoroughly understand your exposures and are supported, prepared, and equipped with the best cyber risk protection plan for your organization.

Discussion of Findings

Decision-Making Process

I Third Party Consulting

It would be wise of companies to enlist the help of third-party consultants when considering purchasing cyber insurance. Consultants and insurance brokers specialize in helping companies thoroughly understand their unique cyber risk profile. To accomplish this, Firm X uses a Governance Process. According to Firm X, "The process we have designed is our strategic advantage. As consultative and strategic advisors, we have built [Firm X]'s domestic center of excellence for Cyber solutions. We facilitate a process that brings the key C-suite stakeholders together, which leads to a collaborative approach toward Cyber with [Firm X] as a core component to your understanding and approach to your Cyber risk." Consultants and insurance brokers also specialize in tailoring an insurance program to fit the needs of a company. And to do this, Firm X uses a Three-Step Approach. According to Firm X, "A sound cyber risk management plan protects your balance sheet, preserves your reputation, and enables growth in your organization. That's exactly what our three-step approach is designed to accomplish." Companies can attempt to replicate the Governance Process and Three-Step Approach internally, but according to Respondent ©, "some companies could probably do this internally, but I imagine most would be better off using a third party (I.e., consultant/broker) to help them navigate and assess their situation." I believe that through enlisting the help of third-party consultants, the decision-making process that companies use will improve as companies will be

receiving expert help. In the words of Stephens (2020), it is my belief that this insight "will help businesses to better allocate their budget appropriately, as they will know what risk their cyber security spend will mitigate, how much cyber insurance they need to buy and what residual amount is within their appetite to retain" (p. 14). This theme is important because it provides a new understanding of how to conduct decision-making. When companies enlist third party consultants, notions such as "it is hard to specify what an insured wants to be covered from" (Carfora et al., 2018, p. 202) could be dissolved." Enlisting third party consultants can help every company that could benefit from risk transfer.

II Augmenting Awareness, Education, and Communication

It would be wise of companies to augment their cyber risk awareness, education, and communication efforts before purchasing cyber insurance. Employee training, testing, seminars, enterprise awareness are important in increasing cyber risk awareness. Informed awareness, education, and communication efforts will make it easier to navigate the hectic market. According to Respondent ®, “Rarely have I seen an organization fully understand their cyber exposure until after they experience an event”. This cyber threat environment is difficult, and instead of waiting for the possibility of an attack to occur, it is important to prepare for this early through awareness, education, and communication efforts. In addition, Media coverage of cyberattacks can also play a role in shaping risk perception. This can instill worry in decision-makers and executives causing them to purchase insurance impulsively, but through awareness, education, and communication efforts, these fears can be lessened. This theme is important because it provides a new understanding of how to conduct decision-making.

III Understanding Needs and Risks of the Company

Understanding the needs and risks of the company is important before buying anything. It is especially important to understand this because buying cyber insurance can be impulsive. Understanding the risk profile of the company is a necessary component of the decision-making process because this helps the decision-makers understand what it is the company wants to invest in. Understanding risks and exposure with an insurance broker can be especially helpful as to not overspend on premiums especially when premiums are being priced rather conservatively. This theme is important because it provides a new understanding of how to conduct decision-making. Taking an enterprise risk management approach will surely help in evaluating needs and risks and planning a course of action when investing in cyber insurance.

Adverse Selection

I Straightforwardness, Reputability, and Trust

Many insurers are using sophisticated technology to overcome adverse selection, but nobody seems to be asking the obvious question of how companies can be made more willing to release information. Majuca et al. (2006) and Shackelford (2012) amongst other works in the literature note that premiums can be reduced if companies have specific security measures in practice. This may then incentivize buyers to purchase a policy. However, this does not completely answer the research question because this approach incentivizes buyers—it does not extract any additional information from them. To answer this question, if insurers want to make impact determination easier, the best way to alleviate this information-sharing barrier is simply to be straightforward, reputable, and trustworthy with potential buyers. This involves being focused on what is most important to the decision-makers. This theme is important as it provides a new understanding of how to alleviate the information-sharing barrier.

Concluding Remarks

Limitations

There are a few limitations of this inquiry. Case studies create room for bias. Firm X is a major insurance brokerage firm, and so it would come as unsurprising when I found that many respondents employed by the Firm suggest enlisting the help of third-party consultants during decision-making. The importance of third-party consultants may be overemphasized.

Another limitation of this study is that I received a small number of responses. Given this limitation, I knew that this audience would not be representative, and so no sweeping generalizations can be made about the themes. My audience was a professional audience, and so perhaps allowing my questionnaire to be open longer would have yielded more responses.

Another limitation of this study is that while qualitative interviews were envisioned by Tøndel et al. (2015), I instead used a questionnaire to gauge and collect responses. Interviews may have yielded more qualitative results and may have provided a deeper understanding of the case being studied.

Recommendations

In concluding my inquiry, future research should try to address the limitations of my study. Since I conducted a case study of an insurance brokerage firm, I think it would be important to conduct a study in which a similar method design is used, but the only difference would be the audience. Instead of questioning an audience that is from the same firm or an audience of the same practice, future researchers may want to confirm my results by questioning policyholders and professionals with more diversified backgrounds. Researchers may want to ask them the same questions to see if results are roughly the same or if new themes emerge. In addition, perhaps instead of conducting questionnaires, future research may want to conduct interviews. This would certainly provide more detailed responses.

Summary

This inquiry explored how the corporate decision-making process can be better conducted and understood in helping the buyer purchase a policy. This inquiry also explored how adverse selection can be alleviated to make the issuance of a policy easier for the insurer. I asked the questions: How can the decision-making process be better conducted and understood to help the buyer purchase a policy, and how can adverse selection be alleviated to make the issuance of a policy easier for the insurer? Respondents seem to agree that the decision-making process can be better conducted and understood if companies ① enlist the help of third-party consultants, ② augment their cyber risk awareness, education, and communication efforts, and ③ improve their understanding of their needs and risks. Should adverse selection be alleviated, respondents seem to agree that insurers ought to be straightforward, reputable, and trustworthy with potential buyers. Each of the themes I found contributed to adding insight into a market knowledge gap. Having reached the end of my inquiry, these themes are not merely themes, but they are pointers to potential solutions to these original research questions.

References

Adivsen. (2013, October). 2013 information security, cyber liability & risk management. https://www.zurich.com/en/knowledge/topics/cyber-and-data-risks/2013-information-security-cyber-liability-risk-management

Bandyopadhyay, T. (2012). Organizational adoption of cyber insurance instruments in IT security risk management– a modeling approach. SAIS 2012 Proceedings, 23-29. https://aisel.aisnet.org/sais2012/5

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009, November). Why IT managers don't go for cyber-insurance products. Communications of the ACM, 52(11), 68-73. https://doi.org/10.1145/1592761.1592780

Baribeau, A. G. (2015, July/August). Cyber insurance: The actuarial conundrum. Actuarial Review Magazine, 42(4), 3-60. https://ar.casact.org/magazine_issues/july-august-2015/

Betterley, R. S. (2010, September). Understanding the cyber risk insurance and remediation services marketplace: A report on the experiences and opinions of middle market CFOs. http://betterley.com/samples.php

Bolot, J., & Lelarge, M. (2009). Cyber insurance as an incentive for internet security. In M. E. Johnson (Ed.), Managing information risk and the economics of security (pp. 269-290). Springer. https://doi.org/10.1007/978-0-387-09762-6_13

Carfora, M. F., Martinelli, F., Mercaldo, F., Orlando, A., & Yautsiukhin, A. (2018). Cyber risk management: A new challenge for actuarial mathematics. In M. Corazza, M.

Durbán, A. Grané, C. Perna, & M. Sibillo (Eds.), Mathematical and statistical methods for actuarial sciences and finance: MAF 2018 (pp. 199-202). Springer. https://doi.org/10.1007/978-3-319-89824-7_36

Cybersecurity & Infrastructure Security Agency. (n.d.). Cybersecurity insurance. https://www.cisa.gov/cybersecurity-insurance

Cylinder, H. (2008). Evaluating cyber insurance. CPCU EJournal, 61(12), 1-19. EBSCOhost.

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

Eling, M. (2020). Cyber risk research in business and actuarial science. European Actuarial Journal, 10(2), 303-333. https://doi.org/10.1007/s13385-020-00250-1

Fernandes, D. (2014, February 17). More firms buying insurance for data breaches. The Boston Globe, Business section. https://www.bostonglobe.com/business/2014/02/17/more-companies-buying-insurance-against-hackers-and-privacy-breaches/9qYrvlhskcoPEs5b4ch3PP/story.html

French, C. C. (2018, April 13). Insuring against cyber risk: The evolution of an industry (introduction). In 2018 symposium insuring against cyber risk: The evolution of an industry [Symposium]. Penn State Law Review, K&L Gates Center, Pittsburgh, Pennsylvania, United States. https://elibrary.law.psu.edu/fac_works/377/

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. Communications of the ACM, 46(3), 81-85. https://doi.org/10.1145/636772.636774

Herath, H. S.B., & Herath, T. C. (2011). Copula-based actuarial model for pricing cyber-insurance policies. Insurance Markets and Companies, 2(1), 7-20. https://businessperspectives.org/journals/insurance-markets-and-companies/issue-196/copula-based-actuarial-model-for-pricing-cyber-insurance-policies

Majuca, R. P., Yurcik, W., & Kesan, J. P. (2006). The evolution of cyberinsurance. ArXiv. https://arxiv.org/abs/cs/0601020

Marotta, A., Martinelli, F., Nanni, S., & Yautsiukhin, A. (2015, November). A survey on cyber-insurance. https://www.iit.cnr.it/sites/default/files/TR-17-2015.pdf

Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber-insurance improve network security? A market analysis. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, 235-243. https://doi.org/10.1109/INFOCOM.2014.6847944

Ponemon Institute. (2011, June). Perceptions about network security. https://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: Insights and implications. Healthcare, 8(2), 133. https://doi.org/10.3390/healthcare8020133

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? Business Horizons, 55(4), 349-356. https://doi.org/10.1016/j.bushor.2012.02.004

Shields, C. (2019, November 15). Cyber insurance: What does it cover and do you need it? Ntiva. https://www.ntiva.com/blog/cyber-insurance-what-does-it-cover-and-do-you-need-it

Shukla, G. (2018, December 31). Amid rising cyber-attacks, data breach, here's how cyber risk insurance can help firms mitigate risk. The Financial Express. https://www.financialexpress.com/industry/amid-rising-cyber-attacks-data-breach-heres-how-cyber-risk-insurance-can-help-firms-mitigate-risk/1429524/

Stephens, S. (2020). How cyber insurance can still leave you vulnerable to risks. Computer Fraud & Security, 2020(2), 12-14. https://doi.org/10.1016/S1361-3723(20)30018-X

Toregas, C., & Zahn, N. (2014, January 7). Insurance for cyber attacks: The issue of setting premiums in context. https://cspri.seas.gwu.edu/publications

Tøndel, I. A., Meland, P. H., Omerovic, A., Gjære, E. A., & Solhaug, B. (2015, November). Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research (Research Report No. SINTEF A27298). https://sintef.brage.unit.no/sintef-xmlui/handle/11250/2379189

Questionnaire

Cyber Insurance: Insights into the Decision-Making Process and Information Sharing Barrier

Informed Consent

You are being asked to participate in a research project entitled, “Cyber Insurance: Insights into the Decision-Making Process and Information Sharing Barrier”. This research is being conducted by [redacted], an AP Research student in [redacted]. The goals of this research project are to (1) gain insight into how the decision-making processes companies use when considering cyber insurance should be improved and (2) gain insight into how the information sharing barrier between the insurer and the company can be alleviated.

As a participant in this project, you will be asked to give a response to a series of questions. The entire process will take approximately 10 to 15 minutes.

You have the right to refuse to participate in this study. If you agree to participate, you have the right to change your mind at any time and stop participation without penalty. You are free to skip or refuse to answer any particular question for any reason.

Benefits of Participation
You will receive no direct benefits from participating in this research study. However, your responses may help the researcher learn more about how cyber insurance decision-making should be improved and how the information sharing barrier can be alleviated.

Risks of Participation
There are no foreseeable risks involved in participating in this study other than those encountered in typical day-to-day life.

Confidentiality
The researcher has made every effort to safeguard the confidentiality of the information that you provide. The questionnaire is anonymous and, therefore, will not collect identifiable information such as your name, email address, or IP address. Any and all data obtained from this study that can be identified with you will remain confidential and will not be given to anyone without your consent. Additionally, only the researcher directly involved with this project and his teacher will have access to the data collected.

Contact
If at any time you would like additional information concerning the project, you may contact the researcher’s teacher, [redacted], at [redacted] or [redacted].

Electronic Consent
You may print a copy of this consent form for your records. Clicking on the “Next” button indicates that you agree to the following statements:
- I have read the above information.
- I voluntarily consent to participate in this research.
- I have, to the best of my knowledge and belief, no physical or mental illness or weakness that would be adversely affected by my participation in the research.
- I am at least 18 years of age.

Demographics

The purpose of this section is to understand some of your basic demographic information.

1. What is your age group?

Mark only one oval.

- ◯ 18-24
- ◯ 25-34
- ◯ 35-44
- ◯ 45-54
- ◯ 55 or older

2. To which gender do you identify?

Mark only one oval.

- ◯ Female
- ◯ Male
- ◯ Other: _____

3. Are you of Hispanic, Latino, or Spanish origin?

Mark only one oval.

- ◯ Yes *Skip to question 5*
- ◯ No *Skip to question 4*

4. Which of the following describes you?

Check all that apply.

Check all that apply.

- [ ] American Indian or Alaskan Native
- [ ] Asian
- [ ] Black or African American
- [ ] Native Hawaiian or other Pacific Islander
- [ ] White or Caucasian
- [ ] Other: _____

Background

The purpose of this section is to understand some basic background information.

5. In or near what metropolitan area is your company located?

_____

6. What industry describes your company's industry focus?

_____

7. Does your company have an insurance policy specifically for cyber risk coverage?

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Unsure
- ◯ Other: _____

8. In what field is your profession?

Mark only one oval.

- Information Technology (IT)
- Insurance
- Risk Management
- Other: _____

9. How many years of experience do you have in this field?

_____

10. What is your job title or profession? You may also provide your seniority level.

_____

Questions

This is the main section of the questionnaire. Please try to answer as many questions as possible.

11. What can insurance companies do to increase the willingness of companies to share security information with them prior to contract establishment?

_____

_____

_____

_____

_____

δ 12. How can insurance companies gain the trust of a company to discuss possible threats to which the company is exposed to or to discuss confidential security accidents?

SG 13. How should companies improve the ways by which they make cyber insurance decisions?

α 14. What decision process or model should companies use when deciding to purchase cyber insurance, and why?

SG 15. How should companies better conduct a self-assessment of their unique cyber situations to navigate the confusion of cyber risk exposure?

β 16. Do cyber risks and the evaluation of cyber risk exposure differ from other areas of insurance?

Mark only one oval.

- Yes *Skip to question 17*
- No *Skip to question 18*

β 17. If yes, how should buyers of policies approach cyber risk?

Skip to question 19

β 18. If no, should insurance companies approach cyber risk in a similar fashion as other areas of insurance?

Mark only one oval.

- Yes
- No

Questions

This is the main section of the questionnaire. Please try to answer as many questions as possible.

Y 19. Having holistic cyber risk management programs to complement traditional risk transfer provisions is an area where buyers and insurers need to work together to maximize the benefits of cyber insurance products.

Mark only one oval.

- ◯ Strongly Agree
- ◯ Agree
- ◯ Undecided
- ◯ Disagree
- ◯ Strongly Disagree

Y 20. Augmenting cyber risk awareness is an area where buyers and insurers need to work together to maximize the benefits of cyber insurance products.

Mark only one oval.

- ◯ Strongly Agree *Skip to question 21*
- ◯ Agree *Skip to question 21*
- ◯ Undecided *Skip to question 22*
- ◯ Disagree *Skip to question 22*
- ◯ Strongly Disagree *Skip to question 22*

SG 21. How can a company's cyber risk awareness be augmented?

Questions

This is the main section of the questionnaire. Please try to answer as many questions as possible. The questionnaire will end once you click on the "Submit" button.

22. How can policy terms be communicated in an effective manner to those roles that are typically involved in making cyber insurance decisions?

23. What actuarial data is most needed when it comes to cyber attack/incident costs?

24. What standardized metrics are most useful for evaluating cyber risk and cost?