Université de Montréal

Cyber Insurance as a Risk Manager

Par
Claudio Modica

École de criminologie
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieurs
en vue de l'obtention du grade de Maîtrise en Science (M.Sc.) en criminologie

Septembre, 2018

RESUMÉ

L'objectif de cette étude vise à comprendre comment les compagnies d'assurance Canadienne conceptualisent les cyber risques afin d'être en mesure de quantifier des pertes résiduelles ou en constante évolution. Par l'entremise de 10 entretiens qualitatif avec des professionnel de l'assurance, nous avons trouvé que la souscription à une cyber assurance peut aider les entrepreneurs à gérer les risques causés par la cyber criminalité. L'étude montre que la cyber assurance contribue à la compréhension et à la diffusion de connaissance en matière de cybercriminalité. Ceci est facilité par la recherche continue sur le phénomène et de la mise à jour ces polices d'assurance. Aussi, il a été trouvé que les professionnels de l'assurance facilitent l'application des mesures de prévention cyber. Cette gestion est permise grâce aux outils mis à disposition des assureurs afin d'évaluer les composantes de sécurité pour contrer les cyber attaques. Finalement, la recherche démontre que le milieu des assurances joue un rôle d'envergure dans la surveillance et la gouvernance des cyber risques.

Mots-clés: ASSURANCE, CYBERCRIMINALITÉ, RISQUE, DONNÉES, POLICE D'ASSURANCE, CYBER ASSURANCE, GESTION DU RSIQUES, THÉORIE ANCRÉE.

ABSTRACT

The goal of this research is to understand how Canadian insurance companies conceptualize cyber risks to quantify a residual or evolving loss. Through ten qualitative semi-structured interviews conducted with insurance professionals throughout Canada, we found that the purchase of cyber coverage contributes to the risk management efforts. Companies are increasingly looking to implement or enhance their cyber security measures through cyber insurance. In fact, the study found that cyber insurance can serve three purposes. The first is that it allows for a better understanding and diffusion of knowledge through the continuous research on cybercrimes and the revision of cyber policies. The second finding is that insurance professionals work with companies to assess and facilitate the integration of preventive measures. This is based on the tools they use to asses a company's cyber security infrastructure. Finally, the study found that insurance companies have a considerable societal impact on the surveillance and governance of cybercrimes.

Keywords: INSURANCE, CYBERCRIME, RISK, DATA, COVERAGE, CYBER INSURANCE, RISK MANAGEMENT, GROUNDED THEORY.

TABLE OF CONTENTS

ABBREVIATIONS

AIG: American International Group

AMF: Autorité des Marché Financiers

CEO: Chief Executive Officer

CSO: Chief Security Officer

CISO: Chief Information Security Officer

CGL: Commercial General Liability

D&O: Director and Officers

DDoS: Denial of Service Attack

DSS: Decision Support System

E&O: Error and Omission

GT: Grounded Theory

IBC: Insurance Bureau of Canada

IRM: Integrated Response Management

ISACA: Information System Audit Control Association

ISO: International Organization for Standardization

IT: Information Technology

MGA: Managing General Agent

OSFI: Office of the Superintendent of Financial Institutions

PIPEDA: Information Protection and Electronic Documents Act

PWC: PricewaterhouseCooper

SCIC: Semantic Cyber Incident Classification

SIN: Social Insurance Number

SMB: Small Medium Businesses

UBPP: Utility Based Preferential Pricing

U.S.: United States of America

U.S.A: United States of America

ACKNOWLEDGEMENT

Writing this thesis was not a simple task and would not have been possible without a strong support team. I would like to take this opportunity to express my gratitude to those who have helped me along the way. Professor Benoit Dupont, thank you for your advice and guidance on what has been an rewarding experience. To my family and significant other, thank you for your unparalleled support and for motivating me when I needed it most.

INTRODUCTION

PlayStation, Target, Home Depot, Ashley Madison and JPMorgan Chase were all victims of cyber attacks. These attacks have not only exposed the companies' vulnerable security measures but also compromised considerable amounts of customers' personal information. As a result, cybercrimes came under a substantial amount of scrutiny from media outlets which, in turn, created interpersonal fear among online users and pushed companies to consider different strategies to strengthen their security measures. Moreover, targeted companies, including those noted above, have found themselves with several class action lawsuits and millions of dollars in restitution to pay their clients. These financial consequences may explain why a company like PlayStation has turned to insurance companies for indemnification for their losses. Yet, several policy complexities have made it possible that insurance companies are not legally obliged to pay for all losses incurred from a cyber attack. (see *Sony Corp. of America vs. Zurich American Insurance Co.*).

Several reasons were outlined as to why Zurich did not have to pay for the losses incurred. Amongst these reasons, Yu (2014) noted that the commercial general liability (CGL) did not consider cybercrimes as a tangible loss. Research also argued that the innovative nature of cybercrimes prevents insurance companies from having the data they need to provide adequate coverage for their clients (Shackelford, 2012; Drouin, 2014). Gordon, Loeb and Sohail (2003) also mention that there is an uncertainty of the markets covered by these cyber insurance policies. Based on these suggestions, risk theorists, such as Beck (1992), are concerned that major technological events are uninsurable (Beck, 1992). According to Ericson and Doyle (2004), uncertainty is defined as "the lack of secure knowledge about an unwanted outcome. Insecure knowledge is a result of unavailable or unreliable data about frequency and severity" (p.12). For Beck (1992)

major technological catastrophes are not restricted to the time and space of the incident. Rather, the origin of such uncertainties extend beyond physical space. In their nature, the afflictions produced by cyber attacks are not tied to a physical space. The prescriptive concept of accident and medical insurance does not adequately fit with the basic dimensions of modern threats. Despite these suggested limits, Ericson and Doyle (2004) argue that each business line of insurance, whether it is commercial, home or life, are facing issues with the availability of scientific knowledge, underwriting practices, loss prevention approaches and claims management. To address these limits, each business line requires "different approaches to risk, attributions of responsibility for risk, and abilities to respond to uncertainties" (Ericson and Doyle. 2004, p.19). New global risks, such as cybercrime, may be difficult to evaluate. The insurance industry can no longer rely entirely on conventional actuarial and risk analysis processes. Thus, the objective of this research is to understand how Canadian insurance companies conceptualize cyber risks to quantify a residual or evolving loss. This research will analyze the practices of insurance companies used to deal with the uncertainties of cybercrime to insure their clients. By doing so, this will help us to determine the challenges faced by different actors in the insurance industry, the divergent opinions on the matter and the techniques used to manage this new form of risk. The research will use a qualitative approach by conducting ten semi-structured interviews with insurance professionals.

The first chapter of the research, the literature review, will explore the fundamentals of traditional insurance and cyber insurance and its place in the risk society. Additionally, this section will also look at the difficulties encountered by insurance professionals when dealing with cybercrime coverages. Following this assessment, the second chapter will be dedicated to the methodology. As previously mentioned, the Grounded Theory was favoured in order to find knew

concepts of cyber insurance products and their pertinence for risk management. It will also describe how the Grounded Theory was applied to extract significant information during the analysis of the interviews.

The third chapter will present the data extracted from the interviews. This section outlines the categories that emerged from the perspectives of insurance professionals. Divided in five categories, this chapter will define cyber insurance, the wording used in policies, the difficulties with the lack of data, the necessity of information networks and finally the cyber resiliency that this coverage offers.

The fourth chapter will analyze the categories that emerged from the interviews and draw a parallel with the information found in the literature review. The analysis will be based on three ways in which the insurance industry acts on cybercrimes. The three means are Understanding Cybercrimes, Risk Management and Behavior Towards Risk. Finally, the last part will look at the Surveillance and Governance of cybercrimes facilitated by the insurance industry.

CHAPTER I: LITERATURE REVIEW

The internet is continuously facilitating how firms conduct their day to day activities. Due to the internet, a company can maximize their efficiency, expand their market to a global audience, and coordinate employees that are working from different locations. In addition, the internet has allowed the development of new business models and services. Examples include online shopping, the selling of domain names and the rental of virtual infrastructures, such as cloud computing. As business owners shift merge to a virtual infrastructure, they expose themselves to new risks, such as cybercrimes, in addition to the traditional liabilities, such as fires, floods and burglary. For this reason, cyber insurance is becoming one of the most sought out coverages by business owners (Insurance Institute, 2015).

Theoretically, risk is continuously present in our daily activities. A risk can only be considered a risk when we, as a society, identify and perceive certain events as detrimental to our operations (Garland, 2003). For this matter, the risk becomes something that needs to be accepted, challenged, eliminated or, when possible, mitigated (Elliott, 1960). In fact, insurance is one of the most important tools to mitigate the effect of a loss (Riegel, Miller & Williams, 1976). In its most simplistic form, risk mitigation through the means of insurance has two aspects. The first is the transfer of a risk. This consists of transferring that risk from the insured to the insurer who has the financial means to pay the loss (Rejda, 2011). The second is the sharing of losses. This concept relates to a group of persons agreeing to pay a certain premium for a common risk they share in order to reimburse the one that may suffer the loss (Riegel & al., 1976).

The previous paragraph offers an overview of the insurance industry services as a risk mitigation product. However, their implication within our modern society go well beyond financial compensation and risk spreading. Several authors have documented their understanding of

insurance. According to Ewald (1991), it's a model of rationality in which it breaks down, rearranges and orders certain elements of reality, which is later formalized through the calculation of probabilities. Baker and Simon (2002) believe that beyond spreading risk, insurance takes part in different activities. For example, Baker (2003) explains that the classification of risk puts forward a vision of individual responsibility and protection. Heimer (2003), suggests that insurers are moral actors and through their contracts, political policies and disciplinary mechanisms, will influence their client's behavior. She advances that through these mechanisms, we should seek to understand insurers' behaviors which also make up insurance relationships.

The first part of this literature review reveals how technologies of insurance calculate, regulate and manage the risk, from a social science perspective. This will be done by understanding the following sections: Origins and Principles of Insurance, the Insurance and Risk Calculation, Insurance as Construction of Social Behaviors Towards Risks, and to conclude, Insurance and Governance.

Following a rather theoretical approach to insurance, the second part will examine a technical facet of the cyber insurance market and its various obstacles. This section will comprehensively look at E-Perils and how they are interpreted legally by insurance companies. It will continue with an analysis of difficulties caused by the absence of data needed to offer competitive cyber coverage.

1. Fundamentals of Insurance

1.1. Origins & Principles of Insurance

As explained by Hacking (2003), insurance is an important institution that allows to get a better understanding of risk and uncertainty. The researcher argues that insurance is at the core of

the evolution of the science of risk and probabilities. Yet, historically this was not always the case. Origins of insurance can be traced back to ancient Rome. According to Vance (1908), some historians, such as Malynes (1622), found that to encourage the importation of corn, the Roman emperor Claudius took on the risk of loss due to potential perils at sea. Similar concepts were also identified in Asian countries, such as China and India. Other authors, such as Gandrud (2014) and Hellwege (2016), argue that insurance practices, particularly business insurance practices, were observed in several other European countries, such as Germany, France and Italy. However, no custom insurance contracts are known to have been found from that time in history. For Vance (1908), such agreements represented a rather vague and limited definition of insurance.

Insurance as we know today originated in the 17th century on Lombard street in England to protect marine risks, such as the loss of merchandise and the lives of ships' crew (Hellwege, 2016). This form of insurance, which was developed by the prominent Lloyd's of London, took on the marine risk by getting an underwriter to "prepare a slip, called a bordereau, that was passed from underwriter to underwriter until sufficient names and amounts were attached to cover the full risk, at which time the insurance was bound" (Prefer & Klock, 1974, p. 17). Additionally, the Great Fire of London (September 2nd, 1666) also contributed to the development of fire insurance (Hellwege, 2016). In 1666, over a quarter of the buildings in London were burned, which prompted Nicholas Barbon to design an insurance contract that is still used today; it allowed insurance companies to restore or replace the damaged buildings (Prefer & Klock, 1974).

These cases paved the way to a specialized insurance industry, as known today. Other than marine and fire insurance, several products are now offered by the industry to assist a company's risk management efforts. As an example, property and casualty insurance covers incidents pertaining to automobiles, burglary and theft. Within this line of insurance, we find commercial

insurance: products geared towards businesses, non-profit organizations and government agencies (Vaughan and Vaughan, 2003). These products are classified in different categories, such as General Liability Insurance (CGL), which is usually a package product that covers basic legal liabilities, property damage and bodily injuries; Director and Officers (D&O), which provides protection to businesses if they are sued due to their directors' or officers' mismanagement of the company they serve; equipment breakdown insurance, which covers the accidental breakdown of specialized machinery; and Crime Insurance, which covers the loss of money and other property due to acts of theft, burglary and other criminal misconduct (Redja, 2011).

These products, are generally understood as a "social device for eliminating or reducing the cost to society of a certain type of risk" (Mowbray, Blanchard and Williams, 1979, p.1). For example, it can compensate for financial losses caused by fire, frauds or cybercrime which led to legal liabilities, destruction of equipment or the temporary shut down of business operations. However, insurance takes on a much larger role than the one defined above. For, Ericson, Doyle and Barry (2003), insurance represents an institution of applied knowledge and social necessity. The researchers believe that the insurance companies' understanding, and governance of risk have a considerable social implication for the development of preventive measures, compensations for losses, social planning and the freedom to take risks. This is achieved through latest knowledge, tools and technologies to develop contracts, premiums, and the development of preventive measures (Ericson and Doyle, 2004). Interestingly, due to their ability to assess risk, some researchers argue that the industry is contributing to the production of risk in parallel. Beck (1992) believes that the scientization of risk contributes to the industry's profits. By defining risks, insurance companies can capitalize on this new form of social fear. Furthermore, Beck (1992) states the following: "risks can be more than just called forth, prolonged in conformity to sales

needs, and in short manipulated. Demands, and thus markets of a completely new type can be creating by varying the definition of risk, especially demand for the avoidance of risk, open to interpretation, causally designable and infinitely reproducible" (p.56). Similarly, Becker (1992), argues that risk is "the probabilities of physical harm due to given technological or other processes. Technical experts are given pole position to define agendas and impose bounding premises as a priori to risk discourses" (p.3). The following paragraph will study the literature about how insurance companies manage risk and, in turn, makes the risk calculable.

1.2. Insurance & Risk Calculation

For Beck (1992), risk is defined as "a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself. Risks are consequences which relate to the threatening force of modernization and to its globalization of doubt. They are politically reflexive" (p.21). Consequently, a systematic way of dealing with risk is insurance. Insurance according to Hacking (2003), is a prominent institution that simultaneously facilitates the understanding of risk and uncertainty while also contributing to the development of the science of risk and probabilities. It is evident that the insurance industry is an institution motivated by capital gains. Heimer (2003), advances that insurers are simultaneously financial institutions and risk managers. In fact, investments profits deriving from the stock market are much more important than profits that result from underwriting the risk (Heimer, 2003). Despite this greater interest in their investment portfolio, insurance remains an important tool to mitigate the loss caused by risks. This is done by attributing itself the responsibility of quantifying, commodifying moral commitments within underwriting practices, preventive security and indemnification (Ewald, 1991). These practices, according to Ericson, Doyle and Barry (2003) assign insurance companies the responsibility to act

on risk and in turn create a social necessity. The researchers continue their argument by stating that decisions taken by insurance professionals will have considerable societal implications that will influence a business owner's decision on the operation of his capital, loss prevention measures, social planning and freedom to take risks. To do this, "insurance will call upon the latest science regarding each risk they are addressing in order to specify the insurance contract conditions and premium rates, assess the validity of claimed losses, and organize loss prevention measures. Ideally their own actuarial science, converts myriad of risk in the world into insurance technologies that spread and compensate losses with fairness and efficiency" (Ericson & al., 2003, p.5).

Ewald (1991) believes that the insurance industry will objectify anything that can potentially be perceived as a risk. For Beck (1992) and Garland (2003), these practices are contributing to determining and legitimizing the risk. In fact, a risk that is not known to be manageable is not considered a risk. Garland (2003) adds that "risk is not a first order of things existing in the world" (p.52). Instead, the number of risks present within our modern society is based on perception and assessment we make on our relationships with certain events that can potentially impact our plans, interest or well-being (Garland, 2003). This suggests that risk determination by the industry is made possible by mathematical possibilities. These mathematical possibilities are referred as actuarial science (Beck, 2003). Traditionally, insurance companies write policies based on an accumulation of historical data, referring to the law of large numbers. Car insurance, for example, is based on decades of claims made by automotive drivers. The premium and the liability coverage for such insurance is based on microdata, containing several types of information. For example, the type of vehicle, the driver's profile and previous claim history are all considerations for liability coverage (Raphael & Rice, 2002; Insurance Bureau of Canada, 2016). Moreover, insurance is based on the principle of probability. According to

Mowbray, Blanchard and Williams (1979), probability refers to the frequency of an outcome to occur over a long period, thus being repeatable. Riegel, Miller and Williams (1976) also state that when applying the principle of probability, two conditions must be met. The first is that future losses coincide with past and present claims. The second, which is of interest for cyber insurance, is that there must be enough data (the Law of Large Numbers) to issue coverages. The Law of Large Numbers, based on the work of French mathematician Simeon Poisson, states that "as the number of trials increases, the proportion of results approaches the underlying probability" (Mowbray & al., 1979, p.24). For this matter, the function of insurance is "to combine a larger number of risks and thus reduce the degree of risk and hence uncertainty" (Riegel & al., 1976, p. 19). Consequently, this science evaluates the risk based on predefined insurable events, accordingly basing themselves on the concept of probability. Consequently, the insured risk is determined based on economic fluctuations and losses from previous claims. Additionally, to quantify a risk, insurance firms identify probability distributions through statistical and economic expectations (Landsman & Sherris, 2001).

For Ewald (1991), these practices are used to objectify the risk that will make it a normality. The underlying premise is that society will not consider them accidental. Giddens (1990) also proposes that insurance products are purchased not only based on actuarial calculation but fear towards security. These actuarial fears justify actuarial practices to render the risk "normal". Moreover, based on this actuarial science, it is apparent that insurance professionals are influence the risk discourses (Beck, 1992). In fact, the production of risk is achieved as the insurance institutions are organizing, managing and controlling activities perceived as compromising (Beck, 1992). Furthermore, the research suggests that through their practices, insurance institutions contribute to the development of risk classification.

As previously mentioned, the mathematical probabilities are based on the law of large numbers which creates a pool of risk. According to Heimer (2003), risk pools are an organization of clients based on their aversion to risk. Ideally, these pools are composed of individuals who, through the premium, generate lucrative profits for insurers. Similarly, Baker and Simon (2003) show that risk pools are used to "seek collective revenues from each policyholder that will cover the cost of that person's probable losses" (p.73). In this regard, insurance companies will seek customers who are morally responsible, who will take the necessary precautions to minimize risks and who will not submit unjustified claims that could affect the integrity of the pool. After all, the goal of the insurance institutions is not simply to provide indemnity for losses. The primary goal is to use profits from premium revenues to increase profits from investments. Hence, a morally responsible client, dedicated to preventing cybercrimes, will develop of contingency plans for their company and ensure that they meet government regulations. Additionally, the implementation of risk management concepts is also perceived as a morally responsible approach (Yang & Lui, 2014; Gordon, & al., 2015; Insurance Institute, 2015).

To reinforce these practices, insurers will often offer their clients deductions on their premiums or deductibles. On the other hand, clients who do not adhere to these practices, are imposed stringier conditions such as higher deductibles and excluded clauses. For others, there is also the possibility that they cannot benefit from any insurance coverage (Heimer, 2003). For Baker and Simon (2002), these practices are contributing to the maintenance and assignment of social classes. Risk classification will force some to pay more money simply to enter the pool, while others will be completely discriminated from entering (Baker & Simon, 2002; Baker, 2003). However, this logic is effective for the insurer because it allows them to offer attractive products

at a fair price and ensure that their pools are not compromised by individuals who are highly exposed to risk (Heimer, 2003).

The previous paragraphs explained how the insurance industry turns uncertainty into a calculable risk and maintains social classes. Although the techniques can greatly contribute to the science of risk, it comes with certain limits. In addition to risk classification, the literature reveals that moral hazards and adverse selection are two predominant issues for the insurance industry.

1.3. Insurance : Constructing Social Behavior

Risk classification contributes to the construction of social behavior. Generally, moral hazards and adverse selection are studied as ways the insurer shapes the insured behaviors towards risk. However, Heimer (2003), brings forward a compelling argument that the behavior of the insured will also shape the practices of the insurer. Building on risk classification, this section will analyze issues pertaining to moral hazard and it adverse selection. Both these facets are studied, through a criminological perspective, to understand how they influence the insured and insurer.

To begin, moral hazards refers to the "dishonest tendencies on the part of the insured that may induce the person to attempt to defraud the insurance company" (Vaughan & Vaughan, 2003, p. 5). When the insurer underwrites a policy for a client, he requires the former to put in place or maintain an adequate level of security to reduce the possibilities of submitting a claim (Baker, 2003). For example, Eling and Werner (2016) suggest, based on Biener and his colleagues (2015), that companies may adopt optimal cybersecurity protection while being evaluated, but once they sign their policy, they will reduce the cost and level of investment in their cyber protection efforts (Yang & Lui, 2014; Majuca, & al., 2006). According to Vaughan and Vaughan (2003), risk managers can invoke the utility theory. This theory explains that, when a risk manager considers

his revenues, he will look at his risk aversion and will decide that reducing his security investment cost will result in a greater monetary return (Mowbray & al., 1979). In fact, Chief Information Security Officers (CISO) simply ask themselves two common questions before codifying the standards within their companies. The first is, how much will the return on investment be? The second is, "How, on an empirical cost-benefit basis, do we know when to patch, fix or shut down systems and when new vulnerabilities arise"? (Elliot, Massacci & Williams, 2016, p. 82). Ericson and Doyle (2003), argue that this approach is influenced by perception rather than adequate knowledge on probabilities. The authors, based on Huber and his colleagues (1997) continue to argue that risk managers are often not interested in probabilities. This mindset looks to protect against certainty rather than the uncertainty itself. For Taylor (1992), in Ericson and Doyle (2003), this is the result of risk managers preferring to invest in protection that is conventional to their operations. In fact, research showed that organizations will seek coverages for a risk only after it occurred. Looking at cybersecurity investments based on the criteria's cited above, will facilitate the allocation of resources. However, applying a cost-benefit analysis to cyber investments can potentially result in a backlash for a company. One fundamental problem is that investing in cyber security does not result in an immediate cost-benefit. Cyber security is rather a long-term investment that will profit a company when the potential losses are limited thanks to an optimal level of security (Gordon, Loeb, Lucyshyn & Zhou, 2015).

To counter this type of behavior the insurance industry will adopt two strategies. The first is to shift the responsibility of the risk to the pool of insured by increasing the cost of premiums while reducing the coverage (Ericson and Doyle, 2003). This, according to Ericson and Doyle (2003), contributes to the risk classification discussed in the previous section, as some individuals will not be able to afford any protection whatsoever. In fact, by using this strategy, the insurance industry

continues to strengthen social inequalities. These disparities are achieved by "assessing who are normal people for inclusion in an insurance risk pool, and who should be de-selected and un-pooled, insurance technologies create morally based social distinctions, hierarchies, and exclusions" (Ericson and Doyle, 2003, p.319).

In addition to strengthening social inequalities, this first strategy also leads to adverse selection. Adverse selection refers to "the tendency of persons with a higher-than average chance of loss to seek insurance at standard rates, which if not controlled by underwriting, results in higher than expected loss levels" (Rejda, 2011, p. 26). Baker (2003) adds that adverse selection is the result of low-risk individuals not adhering to an insurance policy, leaving the insurance pools with individuals representing a higher aversion to risk. As it was already argued, the decision to purchase an insurance policy is based on a cost benefit-approach whereby business owners mitigate the costs of investing in security measures by comparing it to the risk of being infected and the total economic loss that an attack could cause to their commercial activities. Using this business approach, there is also a possibility that firms will be more likely to reduce their investments in IT security infrastructures and opt for insurance coverage only if "the risk premium is equal to the expected loss" (Mukhopadhyay & al., 2013, p.23). This form of probability analysis is an important component of how the insurance industry regulates its customers' behaviour to deal with uncertainties, leading to adverse selection. Riegel, Miller and Williams (1976) believe that companies behave in such ways due to two circumstances. The first is that "the elimination of unfavorable consequences may cost too much relative to the potential gain" (2). The second is that some companies can also retain the risk (Riegel & al., 1976). Such a situation occurs, according to the concepts of risk management, as follows: when "the acceptance is believed to be cheaper, the person subject to a risk may decide to accept it" (Riegel & al., 1976, p.9). Moreover,

firms that are reluctant to invest in their own security infrastructures are also more likely to transfer the risk to insurance companies (Mukhopadhyay & al., 2013).

Based on this brief example, it is evident that the insurance industry is strongly influencing the behavior of their clients. By pooling individuals in categories, insurance professionals are hoping to find themselves with morally responsible clients (Baker & Simon, 2003). However, risk classification concepts have shown that this is not always true. In fact, insurance companies, will transfer the responsibility of the risk to other while increasing the premium cost (Baker & Doyle, 2003). It is important to note that such a social divide also favors the upper middle class through the need to maintain business relationships.

The second strategy to counter moral hazards and adverse selection is done through surveillance. Among the different approaches, legal advisors in the insurance industry will draft a contract that stipulates that clients are liable if they do not maintain the level of protection that was originally in place. Insurance will also offer monetary incentives, in the form of cost reduction, for clients that adopt adequate risk prevention measures (Heimer, 2003). Pal and Hui (2012) also suggest that using tools to monitor their clients will encourage the organizations to expose their security systems and allow the insurer to give advice on what should be done to increase their security. Additionally, if a breach occurs, the insurer will need to analyze the potential losses that the company will endure and the customers that are affected by the attack. By doing so, the clients will also be notified as the attacked company will need to provide monetary compensation through the money they receive from the insurance company (Pal & Hui, 2012). Conversely Drouin (2004) suggests that this practice can reduce the status quo on cyberattacks, which refers to companies refusing to share that they got breached. As the insurance company must analyze the breach, this can contribute to the implementation of viable security protection products since not only can the

claim be denied by the insurance provider, but it can also deter customers from using their platform for electronic services which do not meet security standards.

Moreover, this type of activity allows all the stakeholders to "foster reflexive knowledge of moral risks useful to all parties in the insurance relationship in the active management of loss prevention and responsible choice in risk taking" (Ericson & Doyle, 2003, p.320).

Despite the benefit of forcing companies to implement certain security measures, this type of practice legitimizes the role of the insurer as surveillance agents. Ericson and Doyle (2003), argue that insurance risk logics are rooted within technologies of surveillance, quantification and classification which allows the objectification of risk. In turn, this allows the insurer to structure moral risk through their actuarial practices and probabilities. By following this approach, insurance seeks to determine which people are considered, by their definition, good or bad. For example, risk management audits refer to the detailed and systematic analysis that determines the needs of an organization regarding the risk they face (Vaughan & Vaughan, 2003).

These tools for Ericson and Doyle (2003b), are used as an alternative to reduce moral risks and to "yield more precise knowledge of moral risks and to justify a crackdown on selected contributors to them" (p.358). According to Ericson, Doyle and Barry (2003), insurance institutions are assigned the responsibility to act according to risk. Their practices will strongly influence the functioning of capital, loss prevention measures, social planning and freedom to take risks. Furthermore, Ericson, Doyle and Barry (2003) suggest that it requires their clients to actively participate in the self-governance of their own risks. Thus, these surveillance technologies are used to manage their population at a distance, similar to law enforcement agencies. To achieve this form of governance, insurers use different tools at their disposal such as questionnaires, audits, credit checks, data matching and private investigations (Ericson & Doyle, 2003). For O'Malley (1992),

in Cauchie and Chantraine (2005), this is what the researcher defines as new prudentialism. New prudentialism is a concept that maintains that crime prevention is transferred from collective risk management to individual management of risk. (Cauchie & Chantraine, 2005). However, in this new way of preventing risk, individuals will once again rely on the cost-benefit and consequences of their actions, which will entail moral hazards. By demanding their clients to be the managers of their own risk, the insurance industry is consequently maintaining the presence of moral hazards. In fact, this can be understood, as Heimer (2003) describes it, as an incentive for clients to cheat. Heimer (2003) argues that insurers impose strict conditions on their clients, but as the risk arises, claimants do not receive the payments they think they are entitled to. It is therefore possible that the insured may not comply with the insurers' requirements.

The research supports that the insurance industry acts as preventive risk managers through indirect discipline of their clients by taking adequate measures to secure their assets. While this surveillance is used to achieve an acceptable loss ratio and to reduce moral hazard, it is important to note that the insurance industry plays an active role in managing the safety and security of our companies. In fact, this role is legitimized by government agencies. Thus, the next section will examine the ways in which private insurance practices extend to the role of government.

1.4. Insurance and Governance

Risk classification and the requirement for companies to incorporate security measures are all ways in which the insurer regulates the insured and his behaviour. (Baker, 2003; Heimer, 2003). In this section, we will examine how government-like practices are legitimized and transferred to insurers as they assume legislators' responsibilities.

Ericson, Doyle and Barry (2003) argue that modernization demands the industry to be increasingly involved in risk management. It is thought that a liberal risk regime is emerging. This

regime asks private corporations and individuals alike to semi-autonomously take the necessary steps to protect against risk (Ericson & al., 2003). Thus, "the state is entwined with the private insurance industry, helping to form the economic, social, legal cultural and political aspect of insurance as governance" (Ericson & al., 2003, p.7). In addition, the government also regulates the industry and its social justice technology function by ensuring that risk pooling techniques are fair, policies are sold at a just price and claims are compensated. Meanwhile, the insurance industry invests heavily in bonds and government securities while offsetting losses that might otherwise have been the burden of the state (Ericson & al., 2003).

In addition to these financial implications, the state has the responsibility to oversee the security of their citizens. With the constant evolution of our society, Beck (1992), argues that social control cannot be solely the burden of the state. He argues that this is because the dissemination of knowledge about modern risks is not limited to government officials. As noted earlier, risk is simply the accumulation of knowledge about a hazard that was previously unknown to society (Ericson & Doyle, 2002). Through actuarial processes and forcing policyholders to increase their security standards, the insurance industry is helping the government to manage the "everyday world of safety and security" (Ericson & Doyle, 2002, p.4). Governments and the insurance industry must work in partnership to develop new insurance markets and risk markets that neither insurance nor government can monitor on their own. (Ericson & al., 2003). For Heimer (2002), this is an important component of the insurance industry and its relationship with government as it provides a strong support to enforce law and regulation. For the most part, insurance will regulate certain activities that the state cannot necessarily enforce (Heimer, 2002). For example, in property insurance, the state requires drivers to purchase insurance before operating a vehicle. Hence, the insurer, through underwriting and actuarial practices, will draft policies that enforce a norm and

expected behavior of the driver (Baker & Simon, 2002). This example shows how the insurance industry becomes a regulator, since their private legislation is legally binding, as is the government legislator. (O'Malley, 1991). Baker and Simon (2001) also agree with this idea that the insurer is amongst one of the most prominent sources of regulatory authority.

This regulatory authority is also determined by the way the insurers discipline their clients. In general, governments are tasked, through law enforcement agencies to enact laws and maintain social order (Baker, 2002). This responsibility is, to some extent, transposed to the insurer. Ewald (1991), considers insurance as a moral technology where their risk appraisal disciplines society. He argues that insurance, as opposed to governments bring a different approach to justice. Rather than the idea of cause, insurance is distributing the risk burden to a collective that will decide to abide from determined rules (Ewald, 1991). Similarly, Baker (2002), argues that for insurance to be successful as a risk management tool, it must be a social responsibility. The researcher continues the literature by stating that, in general, when the product is purchased, the client feels that his responsibility for risk is decreased. However, this should not be the case. Baker (2002), suggests that for insurance to work, policyholders must abide to contract rules.

Heimer (2003), on the other hand, argues that insurers, as risk managers, are the regulators of behaviour while simultaneously spreading risk. The researcher continues to argue that this disciplinary process is consistent with Foucault's (1977) idea that there is a process where discipline is now displaced with punishment. The process favors a reduction of social and financial cost while spreading discipline measures in different private and public institutions. Similarly, it seems that insurance can be considered as a component of the new penology, a concept theorized by Feeley and Simon (1992) (Cauchie & Chantraine, 2005). These scholars, believe that neo-liberalism, which fosters a collective morality, are relinquishing the use of punitive disciplinary

measures. These punitive measures are being substituted by managerial goals which encourage "a safeguarding continuum, which is to say a series of resources to be allocated in according to the degree of control required by the risk profile of penalized individuals, but also in accordance with their cost" (Brion, 2001 in Cauchie & Chantraine, 2005, p.6). Additionally, Heimer (2003) believes that the insurance industry contributes to this disciplinary on three different levels. The first, is by instructing clients to adopt risk reduction practices. Second, it is by pushing through regulations that are enforced by financial means. Finally, the insurer uses actuarial techniques to forecast and indemnify accident and deviant behaviors which will reduce the "social cost of non-normative behavior" (Heimer, 2003, p.285). By imposing these three steps, insurance companies make "the punishment, control or reshaping of abnormal or unacceptable behaviour less necessary" (Heimer, 2003, p.285).

2. The Cyber Insurance Market & its Obstacles

It has been determined that the modern insurance industry has a considerable impact in shaping the social behaviours of their clients and becoming an alternative to risk governance. This section will review the challenges insurers encounter when they are trying to commodify cybercrimes. This will be done by studying E-Perils, Legal Framework and Insurance, and the Absence of Data and Actuarial Modelling.

2.1. E-Perils, Legal Framework & Insurance

One of the main differences that is observed with cyber insurance when compared to others is the insured good. Within this professional practice, considerable debates have emerged regarding the insurability of virtual data. This is because cybercrimes fit with standard losses

observed in other claims. Cyberattacks are relatable to business interruption, additional expenditures, the loss of profits and the cost of hardware replacement (Elliott, 1960). As an example, a company that conducts their commercial activities on the web will not necessarily get their product physically stolen or their office and/or storefront damaged. However, they could very well be victims of a cyberattack, which could damage the infrastructure facilitating the business operations and allow for data to be stolen.

As security threats are evolving at a rapid pace, companies are unable to entirely secure their cyber infrastructures despite the considerable amount of money allocated to cybersecurity. In fact, firms have traditionally relied on antiviruses and antispam software, firewalls and several other tools to secure their electronic data (Pal & Hui, 2012). However, Statistics Canada reported in 2016 that 23996 cyber-related violations were reported to Canadian police services. Additionally, PricewaterhouseCooper (PWC) (2017) reported that 46% of economical frauds in Canada were linked to cybercrimes. The techniques frequently used by the attackers were phishing emails (58%) and Malware, short for malicious software (45%). Similarly, in its 2017 data breach report, Verizon (2017) found that, on a sample of 65 organizations breached, over half experienced some form of hack that included the use of malware and malicious emails (also called phishing tools). Yet, several insurance companies are finding it difficult to protect against such losses as definitions regulating insurance practices have omitted cyber losses (Gordon & al., 2003). This complexity lies with the uncertainty concept found under the risk theory that characterizes the field of insurance. Thus, as the previously mentioned studies indicate, cyberattacks are a recognizable crime but they are perpetrated through different technical means, which make it hard for insurance companies to appraise the loss (Pal & Hui, 2012). Therefore, leading to uncertainty when drafting new policies. Understanding uncertainty faced by cyber insurance, it is necessary to uncover

insurance practices, legal practices and legal vocabulary used in drafting policies. After all, insurance companies develop their products in light of the reality of cyberattacks.

E-businesses have emerged through the development of the internet. Nonetheless, traditional firms have also migrated to a form of e-business. From online shopping, online banking and cloud computing, the presence of businesses in the virtual world has become standard causing stirring debate in the insurance industry as to how to accommodate services. After all, insurance companies, through a first-party risk or a third-party risk, offer physical damage coverage policies to tangible properties but not to intangible properties. Gordon, Loeb and Sohail (2003), as well as Shakelford (2012), all reach a consensus on how to classify cybercrimes. Both research groups agree that first-party risk occurs when there is a loss of profit in line with theft, the trade of secrets or extortion made by hackers. On the other hand, third-party risks are related to damages that are caused to another company by forwarding a computer virus; the inability to provide a service due to cybercriminals stopping the firm's activities; or the theft of credit card information by a third party (Gordon & al., 2003; Shakelford, 2012). However, with different types of business activities taking place virtually, insurance companies are left uncertain whether cyber breaches are considered tangible or intangible (Yu, 2014). According to one author, this ambiguity is caused by the CGL, under which tangible goods are considered physical and are related to property damage. Many computer-based storage facilities and other cyber coverage are, thus, excluded since, "electronic data is not a tangible property" (Yu, 2014, p. 240).

The word tangible is a major concern when drafting insurance policies (Majuca & al., 2006). As previously stated, the wording of insurance policies became a major factor in deciding if virtual data can be considered tangible property. To circumvent court decisions and offer their clients adequate protection, insurance firms have decided to modify their policy vocabulary

(Willis, 2010). For Eling and Werner (2016), this can be done in two distinct ways. The first is by modifying the policies and explicitly excluding cyber losses therefrom. The other is to include them in traditional policies but adjust the premium accordingly. Nonetheless, this approach is not feasible not only because of the CGL but also due to the Insurance Service Office. The Insurance Service Office, an American company offering insurance information and analytics to a global market, takes a limited approach in what it defines as a tangible property. In fact, within their guidelines, they clearly highlight that electronic data is not a tangible property as it is simply information that is stored on various technological equipment, such as computers, software and drivers (Yu, 2014).

2.2. The Absence of Data

A serious problem for the insurance industry is the lack of data on cybercrimes required to develop competitive policies. We know that actuarial calculations are based on historical data, like a common product such as automobile insurance, which represented 42.2% of claims written in 2015. In addition, net claims made by policyholders amounted to more than $15 billion (Insurance Bureau of Canada, 2016). These figures clearly show how the ability to develop car insurance policies is based on available data. This availability is lacking in the cyber insurance landscape.

Historical data is important as it allows the insurer to evaluate the possibilities of an eventual risk. Such practice is not facilitated within the cyber insurance market in Canada as opposed to the American market (Insurance Institute, 2015). This can be explained by the United-States' legal approach to cyberattacks and adverse selection. The cyber insurance market is much more developed in the USA. This is in part due to proactive measures taken by their government. As previously mentioned, in 2002, the American government enacted several laws that require

companies, when they are breached, to notify the public and their clients. These laws have significantly increased cyber security awareness and the demand for cyber insurance (Eling & Werner, 2016). It can also be assumed that a similar trend will be observed in Europe, since the European Parliament and the Council of the European Union have adopted the Directive on Security of Network and Information Systems. These directives, which should be standard across the European member states' laws by 2018, will demand that several industries, such as transport, water, banking, financial market and healthcare systems, "take appropriate security measures and … notify serious incidents to the relevant national authority" (European Union, 2016). Yet, this active participation is absent within the Canadian legal framework. In fact, the Insurance Institute (2015) suggests that the Canadian government may want to expand their role within their Cyber Security Strategy. This would enable the insurance market to acquire additional data regarding cyber incidents making the drafting of policies plausible. Additionally, insurance firms and the government can venture into a partnership that allows for the promotion of cyber security by favouring a preventive and resilient approach (Insurance Institute, 2015). Indeed, it can be argued that if the government forces companies to divulge their cyber incidents, it can allow insurance companies to accumulate a considerable amount of data. In turn, with the vast data accumulated, insurance firms can assist the government in developing a stronger cyber security policy and enhance cyber security tools to prevent any further attacks that can compromise the nation's classified information.

With the continuous transfer to digital services, many businesses are seeking to purchase coverage that will protect them against corporate espionage, attacks that compromise their operating systems or that keep their files hostage (Insurance Institute, 2015). However, most cyber insurance policies available to the Canadian market do not fully cover these losses (Eling &

Werner, 2016). The lack of legal constraints to force companies to divulge their breaches is also a primary factor in the slow development of cyber insurance; it is suggested that, due to the lack of reporting, insurance firms do not possess adequate knowledge and large numbers to anticipate losses (Gordon & al., 2003). In turn, this forces insurance companies to set a price on unquantifiable data, which does not necessarily represent the actuarial value, and which leads to the principle of adverse selection (Gordon & al., 2003).

Several researchers have suggested that it would be wise for companies to expose their breaches to the public. One of the main purposes is to avoid information asymmetry which then leads to an adverse selection. (Biener, & al., 2016; Eling & Werner, 2016). Regarding cyber insurance, information asymmetry arises when clients that seek out cyber insurance policies have already been breached and are withholding that information from their insurer (Gordon & al., 2003; Eling & Werner, 2016). However, as there are not any standard cyber breach measurements developed within the field, insurance firms are unaware if their client's digital infrastructure is considered a high or a low risk in terms of losses (Majuca & al., 2006).

The adverse selection contributes to another consistent problem faced by cyber insurance which also leads to a lack of data. In general, when estimating the loss created by a cybercrime, insurers tend to focus their study on short term direct losses (Insurance Institute, 2015). Yet, it is suggested that before a company learns that they have been attacked several months can go by (Insurance Institute, 2015). In fact, a study by the Ponemon Institute (2015) found that it can take a company up to 170 days to discover an attack, and if an attack is conducted by an insider, this can take over a year to discover. Moreover, since estimating the cost of a cyber attack is often based on short term losses, insurance companies often fail to predict or analyze future impacts of the attack, which goes against the principle of probability. As an example, quantifying the loss of

a laptop is easy to assess, but it can be difficult to estimate the value of data found in the laptop, which may or may not be compromised or which may be revealed only at a later time (Insurance Institute, 2015). Thus, depending on the frequency, severity and value of the loss, the costs that are considered usually account for crisis management, the income lost during the business interruption, and negotiations to pay their customers or extortion fees (Insurance Institute, 2015). This again causes insurance firms to limit their policies and offer a general coverage that only covers certain aspects of attack, such as legal defenses, forensics and notification services if the law requires it (NetDiligence, 2016). However, Majuca and his associates (2006) noted that, if organizations are more likely to divulge their information, this will allow insurance companies to reduce their premiums and offer coverages that respond to the losses created by a cyberattack.

2.3. Actuarial Modelling

Insurance is predominantly based on actuarial science and statistical and economic expectations. However, as previously mentioned, the Canadian legal framework and the lack of data do not facilitate these actuarial techniques. In fact, Eling and Werner (2016) refer to the Law of Large Numbers when they suggest that "the quality of available data also limits the improvements that can be made in modelling. Especially for insurance purposes, the number of data breaches is not sufficient to calculate premiums, capital or reserves" (p.478). To circumvent these limits, Walsh (2001) and Majuca, Yurcik and Kesan (2006) suggest that it is necessary for Risk-metrics to be developed to facilitate the estimation of a risk. To this end, different approaches have been suggested by authors, such as a Semantic Cyber Incident Classification (SCIC) model, a Monopolistic Cyber Risk Probability Measure, a Model of Self-Protection and Utility Based Preferential Pricing (UBPP).

For Elnagdy, Qiu and Gai (2016), cyber insurance represents an effective tool that serves the financial industry to reduce potential cyber risks. Nonetheless, they argue that the lack of data and poorly developed actuarial frameworks can cause an insurance firm to endure important financial losses and make costly actuarial mistakes. If such a scenario presents itself, it would be unreasonable for insurance companies to offer protection against cyberattacks as the objectives of an insurance company are to make their business profitable, compete with other firms and pay claims as they happen (Rejda, 2011). To prevent such failures, Elnagdy, Qiu and Gai (2016) suggest adopting a SCIC model. This model requires actuaries to proceed with an ontological approach consisting of three phases. The first is to understand technical rules and regulations as well as restrictions regarding cyber incidents. The second phase requires the use of ontological definitions that can be observed in phase one. Finally, the third phase involves linking the previous two steps and identifying the different relationships that can potentially lead to a cyberattack (Elnagdy, Qiu & al., 2016). Similarly, Pal and Hui (2012) suggest a Monopolistic Cyber Insurance Model. This model requires each client seeking to invest in cyber insurance to adhere to a determined level of security standards. Following the implementation of these standards, insurance firms assess these measures as well as the location, externalities and quality of the data to develop a policy. Additionally, the insurance firms allocate rebates or fines in their client's premiums if they did or did not maintain the established level of network security (Pal & Hui, 2012).

As opposed to the SCIC and the Monopolistic cyber insurance model, Landsman and Sherris (2001) suggest a model that does not require companies to invest in additional cyber protection. Their model bases itself on statistical and economic assumptions. The researchers consider that individuals are risk averse. Financially speaking, a risk averse individual is, for example, an investor who would rather make a low than a high return while minimizing the risks

associated with their investment (www.investopedia.com). Thus, to determine a premium for a cyber risk, it would be necessary to financially convert probability distributions and random future gains or losses. This would allow insurance firms to set a premium based on certain observed behaviors in the fields of insurance and financial markets (Landsman & Sherris, 2001). However, Bolot and Lelarge (2008) believe that only relying on risk aversion is less attractive to insurance firms. This is because when a cyber breach occurs, it is most likely that it will be correlated with other forms of risk. Additionally, by exclusively relying on risk aversion, insurance firms will omit analyses of the potential risks faced by others (Bolot & Lelarge, 2008).

To counter the correlated losses that can be faced by others, Mukhopadhyay and his colleagues (2013) propose a UBPP model. This concept is based on the belief that each organization has its own risk profile. Thus, when calculating the premium and analyzing the risk, four distinct categories are taken into consideration. These categories are the following; the probability of a malicious event, online revenues generated by the organization, and the utility expected from the insured and uninsured customer (Mukhopadhyay & al., 2013). Based on this model, the researchers believe that when analyzing all the variables present in an organization seeking cyber insurance, insurance firms can provide attractive premiums as a guarantee that the payments will be made in case of an attack (Mukhopadhyay & al., 2013).

Some (e.g. Bohme and Schwartz (2010)), moreover, suggest a framework that unifies all the approaches previously mentioned. This framework bases its modelling decisions on five specific factors: the network environment, the demand side, the supply side, the information structure and the organizational environment (Bohme & Schwartz, 2010). The researchers believe that this modelling framework would allow for a better comprehension of cyber risks. In fact, cyber risk models cannot differentiate themselves only through a demand supply approach but, rather,

require a global understanding of cyber networks, information and security standards established by their clients. Additionally, standard information, such as the time and place of an attack potentially taking place, are considered relevant information (Bohme & Schwartz, 2010).

Although these frameworks seem to have a certain appeal to insurance firms, they have several limits. A major one, which is also highlighted by Bohme and Schwartz (2010), is that there was no quantitative data and a lack of correspondence to the probabilities rules. That is, the proposed models were not tested with concrete data but rather test scenarios. The mathematical formulas employed in the calculations of a premium are simply hypotheses made by the researchers. This being the case, it seems rather unlikely that insurance companies would adopt a modelling approach without it being tested on concrete evidence as this can generate considerable uncertainty and losses for the insurance firm if the risk is not properly assessed. Moreover, Garland (2003) argues that the validity of risk assessment tools depends on previous categorization systems and metrics. Yet, with cyber insurance being a new product it seems difficult to apply such actuarial models. Other than the lack of data, these modelling approaches heavily rely on the work of different actors. As an example, the different models that are being proposed suggest that an audit should be made before a premium can be calculated. The audit is administered by insurers, analyzes the company's security parameters and requires them to meet certain standards which are defined by Rejda (2011) as pre-loss objectives. These are recommendations made to companies which require them to deploy adequate cyber security solutions within their organizations. These solutions include the development of contingency plans and insuring that the companies meet governmental regulations. Implementing these risk management concepts can also be an advantage for companies as they can possibly benefit from a discount on their premium (Yang & Lui, 2014; Gordon, & al., 2015; Insurance Institute, 2015).

3. Limits & Context

The literature outlines how the insurance industry acts as a risk management tool and the social implications of their practices. Insurance research is typically geared towards legal and economic studies. However, it is an integral part of social science and an important locus of research for the sociology of institutions. It should be noted that insurance governs other institutions, including the state, due to its power of collecting and diffusing risk. According to Ericson, Doyle and Barry (2003), "the insurance institution is a hub and repository of the risk communication systems of other institutions in defining, production, taking and managing risks" (p.9). Ericson and Doyle (2004) argue that for the insurance industry anything is insurable as long as it falls within the principles of insurability regardless if new risks are brought by the modernization of technologies. It is important to note that the literature was based on traditional products such as life, general and property insurance. To understand how Canadian insurance companies conceptualize cyber risks to quantify a residual or evolving loss, we will bring a new understanding on the techniques used to underwrite cybercrimes, define cyber risk, produce knowledge on risk and the management tools that the insurance industry develops for this new form of risk.

The literature also showed that insurance institutions, through their techniques of defining, producing and managing the risk, create market pools and produce risk. These pools create classifications that maintain social inequalities (Ericson and Doyle, 2003). On the other hand, insurers are also becoming effective risk managers by preventing the spreading of risk. Hence, it is argued that the "private insurance industry helps shape the contour of risk society as we well as the problems faced by that society" (Ericson & al., 2003). For this matter, by interviewing insurance professionals operating in the field of cyber coverage, the research will address the limits

of the scientific knowledge on cybercrime developed by Canadian insurance institutions as well as how they operate within the boundaries of these limits. This will bring added value to the sociology of risk and a better understanding of the role private industries play in helping government agencies and organizations to manage cyber risk.

CHAPTER II: METHODOLOGY

Following these limits, the goal of this thesis is to understand how insurance companies conceptualize cyber risks in order to quantify a residual or evolving loss. This topic is particularly relevant as it will enable an in-depth understanding as to how insurance companies interpret cybercrime and will also provide a better understanding as to how the little data available to them is quantified in order to act as an add on to risk governance. The following chapter will be dedicated to the methodology used within this research, namely, a qualitative approach based on the Grounded Theory methods and techniques developed by Glasser and Strauss (1967).

The first part of this section will focus on methodological choices and how they relate to the research objectives. Additionally, this chapter will cover the data collection which encompasses semi-structured Interviews and Theoretical Sampling. Finally, the chapter will conclude with the techniques used to facilitate the data analysis.

1. Methodological Choices

1.1. The Qualitative Approach & Grounded Theory

Throughout this study, a qualitative approach was preferred as the goal is to better understand how professionals in the field of insurance conceptualize cyber risks. As opposed to quantitative methods, the qualitative approach allows for research participants to better define

"what is central and important in their experience" (Van Den Hoonard, 2012, p. 2). Similarly, qualitative research will enable the exploration of a field filled of studies where little is known about the subject (Strauss & Corbin, 1998). Additionally, qualitative methods are designed to develop an understanding that emerges from interactions between individuals and the meaning they assign to certain factors or events, which in turn leads to the development of a theory (Strauss & Corbin, 1998; Van Den Hoonard, 2012). This is considerably different from quantitative methods as those who use the quantitative approach usually begin with a theory and then conduct empirical tests to verify the validity of such theory (Van Den Hoonard, 2012). Hence, as previously mentioned, the relatively new state of cyber insurance requires the employment of a qualitative approach as barely any data or research is available. Thus, interacting with insurance professionals will facilitate how the former conceptualize cyber insurance.

To facilitate the development of such theory, Grounded Theory (GT) approach, designed by Glasser and Strauss (1967), will be employed as the methodology behind the research. Despite the fact that some, such as Loubster (1968), believe that such an approach is considerably inductive, GT is ideal to analyze cyber insurance as it facilitates the development of theories that can be pertinent to both political and practical analysis (Charmaz, 2014). In fact, GT is far from being inductive; it requires the researcher to start researching without any preconceived theories. Individuals that choose to employ such a qualitative method must continuously gather data and conduct thorough analysis throughout the research process (Creswell, 1998; Strauss & Corbin, 1998). This methodological choice allowed us to understand what is happening within the governance of cyber risk through insurance (Bryant & Charmaz, 2007). Additionally, according to Strauss and Corbin (1998), the use of creativity in developing a theory will force the researchers to "aptly name categories, ask stimulating questions, make comparisons, and extract an innovative,

integrated, realistic scheme for masses of unorganized raw data" (13). Hence, this will allow for the study to resemble with more accuracy the phenomenon that is being observed, which in this case is cyber insurance. In fact, according to Glasser and Strauss in their book *The Discovery of Grounded Theory* (1967), GT allows for systematic and rigorous research procedures that will facilitate the development of conceptual categories.

1.2. Sampling Method

At the core of our sampling method, Theoretical Sampling was used in order to satisfy the requirements of Grounded Theory. Theoretical Sampling refers to the process of gathering participants, which will allow one to maximize the information available, and find categories and concepts to facilitate the development of a theory (Strauss & Corbin, 1998). This approach entails that, going forward with interviews, participants are selected not based on a predefined population but by the emergence of theoretical ideas (Walsh, Bailyn, Fernandez & Glaser, 2015). However, this does not mean that the initial participants will be picked randomly.

For the first part of the selection process, Theoretical Sampling requires researchers to set initial considerations to fit the purpose of the study. The first consideration is to select the group that will be studied. This is directly based on the research question and the field of study. The second consideration requires the researcher to decide what type of data will be used to conduct the research. The choice of data, such as observations, interviews, biographies etc., depends on what is more beneficial to the research. The third consideration requires the researcher to decide how long a field should be studied and if he or she must modify that field as the research progresses. This also depends on data saturation. Finally, the researchers need to consider the

amount of data needed for the study. However, this consideration will be modified as the theory being developed evolves (Strauss & Corbin, 1998).

Based on the preceding considerations, several criteria were decided for the benefit of the research. The first criterion required that all the participants be working within the Canadian insurance market, since the research is based within Canada. Thus, the participants needed to hold different roles within the field of insurance, such as brokers, underwriters, lawyers, claim adjusters, actuaries and customer service representatives. There was no criteria as to the company they worked for. This research tried to get insightful data from professionals who work within different companies whether they are big insurance companies or small local brokerage cabinets. Although individuals had to be working in the insurance market, it was essential that they also possessed an expertise of cyber insurance. This selection was quite difficult as not many professionals specialised in this form of insurance. To facilitate the selection process, several organizations, such as the Insurance Bureau of Canada (IBC) and the Autorité des Marché Financiers (AMF), were contacted to see if they could assist us in finding participants. However, due to the specific nature of the research and their organizational roles, they were not able to help. Thus, LinkedIn became the primary resource to search for participants. Within the social networking website, several filters, such as locations, title, position, interest, field of expertise and company, were selected. As an example, in one general query, Canada was the location, Cyber Insurance was the industry and Underwriter was the position. By this approach, we found 41 professionals who fit the profile of the research. However, LinkedIn was not the only tool used to search for cyber insurance professionals. Certain publications that were analyzed contained contact information for professionals working within the subject of research. These publications came from the Canadian Underwriter as well as company-based publications found on their corporate websites. These

included companies such as Marsh, Northbridge, Zurich, AIG and Chubb. Out of these publications, 7 professionals were identified but only 2 accepted to participate.

Once the interviews started, the second part required by GT and facilitated by Theoretical Sampling came into effect. This approach entailed that interview participants were not selected based on a predefined population but by the emergence of theoretical ideas (Walsh & al., 2015). This was possible due to the fact that, as we progressed in the interviews and analyzed the data, comparing and contrasting had to continually be done in order to develop emerging categories. Additionally, the idea behind this approach was to "confirm or disconfirm the conditions, both contextual and intervening, under which the model holds" (Creswell, 1998, p. 119). By using such a framework, the sampling ended once the research was saturated (Strauss & Corbin, 1998). Saturation is defined as when one researches to the point where collecting new data is counter productive, not adding anything relevant, or when the researcher runs out of time, money or both (Strauss & Corbin, 1998).

1.3. Semi Structured Interviews

To stay true to GT, semi-structured interviews were used to conduct this research and gather the data required for the development of a theory. According to Creswell (1998), when using GT as the methodological approach, one must conduct several visits to the field. Although the methodology does not require any standard qualitative combination of procedures in regards to data collection, it is important for a researcher to continuously analyze the data that is being collected. In fact, the use of a GT approach implies that researchers must follow a zig-zag process. This process requires the interviewers to go out into the field to "gather information, analyze the data, back to the field to gather more information, analyze the data and so forth" (Creswell, 1998;

57). Hence, these interviews were conducted while simultaneously coding, categorizing and analyzing the data that was being collected. However, to insure the fluidity of this section, the coding and analysis steps will be presented in the following paragraphs. The process of interviewing stopped only once the data collected was saturated.

Based on the interviewing requirements while using GT, semi-structured interviewing was selected as it allowed the interviewee freedom with respect to the information they provided (Poupart, 1997). In particular, it allowed the participant to fully and freely express his or her knowledge about cyber insurance, which is what the methodological framework requires (Kvale & Brinkmann, 2009). Of course, the interview did have a script; however, it was developed not to force the participant to answer predisposed questions but to offer structure. In fact, the script had certain guidelines with suggested questions, but the way they were asked depended on the answers given by the participant and potential new directions created thereby. Thus, this interviewing technique facilitated the GT requirement that the interviewee have freedom given that his answers reflect the actual social setting as he understands it, which could differ among participants (Suddaby, 2006).

2. Field Work

2.1. The Participants

Ideally, Grounded Theory requires 20 to 30 participants as such allows for the saturation of data. However, due to the relatively new product of cyber insurance, the lack of professionals specialising in the field in Canada, the non-response rate, and time constraints, the sample size was limited. Based on the criteria dictated by Theoretical Sampling, the population for this study consisted of 10 professionals from different Canadian cities such as Toronto, Hamilton, Montreal,

Vancouver and Calgary occupying different roles in the field of cyber insurance. These roles include underwriters (4), lawyers (1), insurance brokers (4) and claim adjusters (1).

Having insurance actors of different backgrounds is necessary for this research. In fact, it is believed that insurance is a complex organization where the interest of different actors come into play (Heimer, 2003). Heimer (2003), argues that an insurance broker can push for sales of policies to benefit from a monetary incentive. On the other hand, underwriters can refuse a client as he presents himself as a considerable liability for the insurance pool (Ericson & Doyle, 2004). Thus, this research will bring a better understanding of what is conceptualized as a cybercrime by professionals operating in the same field but occupying different positions. Although this is a small sample size, the validity of the data should not be dismissed. For one, most studies conducted within the field of insurance are geared towards legal and economic research, leaving the study of insurance under a social science perspective scarce (Beck, 1992; Ericson & al., 2003). In addition, the social science research consulted in the literature review focused on more traditional insurance products, with minimal reference to cyber policies. Of course, this is explained by the fact that cyber insurance is a relatively new product on the market and its study was not relevant to scholars at the time. Thus, this sample size can be precursor for researchers who wish to continue understanding of cybercrimes and cyber insurance from a social science perspective.

That being said, to get a general understanding of cyber insurance, no preferences were given to the type of company they worked for. Participants worked for internationally recognized insurance companies to small brokerage firms. Additionally, one worked for an independent legal cabinet and another for a claim adjusting company located in Montreal, Quebec. However, no information can be shared regarding the name of the participant and his company. The participants

requested that their information remain anonymous. For a detailed description of each participant, please refer to *Table 1* p.42.

Once the contact information of potential participants was obtained, an initial email explaining the research goal and asking if they were interested in participating was sent. Additionally, a second email was sent if someone did not respond. The response rate was low; we were only able to interview 10 out of the 48 professionals that were contacted. Although this number does not reflect the standards required by GT, the rules of Theoretical Sampling were followed. In fact, during the LinkedIn research, the initial search was made through a Convenience sampling, which is used to find individuals within the field that are likely willing to participate in the study (Bryant & Charmaz, 2007). This first part allowed us to interview three individuals: an underwriter, an insurance broker and a claim adjuster. As the research progressed, and the data was being analyzed, basic themes were emerging from the conducted interviews. This allowed us to guide the search in order to find additional professionals who could contribute to the research. Hence, more underwriters, brokers and claim adjusters were found along with two lawyers. The lawyers were necessary as they explained the legal framework that surrounds insurance and cyber insurance. Nonetheless, the research would have also benefited from participants with other roles, such as call center agents, actuaries, analysts and loss prevention agents. Such persons could have brought additional value to the research as they have diverse responsibilities and play different roles within the market. For example, a loss prevention agent would most likely not use the same tools to analyze a traditional claim as she would to analyze a cyber breach claim.

Table 1

Participant Details					
Participant 1					
Role:	Underwriter	**Gender:**	Male	**Age:**	Unknown
Location:	Toronto, Ontario		**Type of Company:**	International Insurance Company	
Expertise:	- Underwriting Directors and Officers (D&O); - Professional Liability Insurance; - Privacy Liability (Cyber Resource); - Providing Insurance solutions for cyber and privacy needs.				
Participant 2					
Role:	Senior Underwriter	**Gender:**	Male	**Age:**	Unknown
Location:	Toronto, Ontario/Boston, Massachusetts		**Type of Company:**	International Insurance Company	
Expertise:	- Errors & Omissions (E&O); - Security and Privacy; - Promoting his respective companies' E&O offers in Canada; - Creation of Cyber insurance business strategy.				
Participant 3					
Role:	Broker	**Gender:**	Female	**Age:**	32
Location:	Vancouver, British-Columbia		**Type of Company:**	Insurance Brokerage Cabinet	
Expertise:	- Commercial Insurance and Risk Management - Marketing new business in professional liability (E&O), technology insurance, small business insurance and trucking insurance; - Research Managing general agents (MGA).				
Participant 4					
Role:	Lawyer	**Gender:**	Female	**Age:**	Unknown
Location:	Toronto, Ontario		**Type of Company:**	Private Law Firm	
Expertise:	- Fidelity Insurance cases; - Commercial insurance cases; o Professional Liability claims; o CGL; o Business Interruption claims; - D&O.				

Participant 5					
Role:	Broker	**Gender:**	Male	**Age:**	32
Location:	Hamilton, Ontario		**Type of Company:**	Insurance Brokerage Cabinet	
Expertise:	- Professional Insurance and Risk Management Service; - Cyber Liability Expert; - Insurance Brokerage Services.				
Participant 6					
Role:	Claim Adjuster	**Gender:**	Male	**Age:**	Unknown
Location:	Montreal, Quebec		**Type of Company:**	Claim Resolution Services	
Expertise:	- Fidelity and financial institution bonds; - E&O; - Trade Credit Insurance Claims; - Investigation in Professional and Liability Claims; - Managed programs for Claim Handling and Risk Management				
Participant 7					
Role:	Senior Underwriter	**Gender:**	Female	**Age:**	33
Location:	Calgary, Alberta		**Type of Company:**	Canadian Insurance Company	
Expertise:	- Technology & Cyber; - Offers custom cyber solutions to customers; - Private Security Coverage.				
Participant 8					
Role:	Underwriting Specialist	**Gender:**	Male	**Age:**	Unknown
Location:	Montreal Quebec		**Type of Company:**	Canadian Insurance Company	
Expertise:	- Technology Insurance Underwriting; - Manages Technology Portfolio; - Product Development; - General Underwriting (Network & Information Security).				

Participant 9					
Role:	Broker	**Gender:**	Male	**Age:**	27
Location:	Montreal, Quebec		**Type of Company:**	Insurance Brokerage Cabinet	
Expertise:	- Professional and Liability Insurance; - Business Development (Cyber Insurance); Insurance Brokerage Services.				
Participant 10					
Role:	Underwriting Director	**Gender:**	Male	**Age:**	Unknown
Location:	Toronto, Ontario		**Type of Company:**	International Insurance Company	
Expertise:	- Development of National Underwriting Guidelines; - Product Development & Legislation Analysis; - Develops Corporate and Regional Business Plans; - Management of Cyber Risk Insurance Products.				

2.2. Interviewing Process

Despite the aforementioned limitations, times were arranged for telephone interviews with those who answered the email and showed an interest in taking part in the research. These interviews were planned to be only about thirty minutes each, as we did not want to inconvenience the participants. Yet, the interviews lasted well beyond this time. On average the interviews lasted 43 minutes and 44 seconds where the longest lasted 1 hour 2 minutes and 54 seconds and the shortest lasted 34 minutes and 56 seconds.

As previously mentioned, semi-structured interviews were the preferred method as they allowed the participants to fully express their knowledge without any restrictions (Poupart, 199). Most of the interviews (8/10 were conducted over the telephone, because these professionals came from different parts of Canada and in-person interviews were not possible. However, two other interviews were in-person; one participant was from Montreal and the other was from Toronto and on a business meeting in Montreal.

For the research, both types of interviews (i.e., by telephone and in-person) had their advantages, which facilitated the gathering of data. Telephone interviews are theoretically cost effective as the researcher does not have to travel to partake in the research. This also enabled us to reach out to participants located across the country (Opdenakker, 2006). As a result, this allowed us to get a general understanding of cyber insurance across the country rather than just focus within the Greater Montreal Area. Moreover, we believe that the telephone interviews were favoured by the participants as they had the choice to do them in their location of choice. As an example, one of the participants did the interview on his way to meet his client an hour away from his office. We believe that this was an incentive as it allowed him to participate without losing any work time. Another advantage that was noticeable during the telephone interviews was that, often, the

participants would speak about certain insurance applications and articles. To clarify what they were talking about, they would send it to the email address provided as we spoke. This facilitated the discussion as we were able to consult the documents and ask questions if needed. However, certain difficulties were encountered when conducting telephone interviews. Like Carr and Worth (2001) suggested, it was noticed that we were not able to interpret the visual cues given by the participant. As an example, if the interview was too long, it was not possible to evaluate the participant's fatigue. Additionally, it is possible that telephone interviews did not necessarily bring the participant to fully engage in an informal conversation. According to Creswell (1998), an informal conversation can allow the research to gain more insightful information as the participant becomes more comfortable with the interviewer. However, this advantage was not observed with the two one-on-one interviews that were conducted. After both one-on-one interviews, it was determined that they were not practical. In fact, this type of interview technique limited note taking. Even though these interviews were recorded, taking down certain ideas, references or key concepts that could have been explored in the current or future interviews would have been helpful. As per Grounded Theory, modifying the interviews as the data was collected was important as it allowed us to get a better understanding of the subject being studied (Strauss & Corbin, 1998). However, since only some notes could be written down during one-on-one interviews, insights may have been forgotten after the interviews were over.

Regardless of the type of interview, it was essential to show signs of reflexivity and transparency. This was done to build a relationship of trust in order to maximize the data that could be made available (Pérez, Mubanga, Aznar, Aznar, & Bagnol, 2015). This was particularly necessary as several participants worked for well-known insurance companies and wanted to make sure that the information they were releasing would remain confidential. We had, in fact, assured

participants by email as soon as they manifested interest in participating; we had sent them all the necessary details and specifics of the research as well as two documents. The first document explained the confidentiality of the research, and the second document was a consent form that gave us the right to use the information provided. The consent form also mentioned that the participant could withdraw from the research at any moment. Nonetheless, no withdrawals occurred.

To begin an interview, a phone call at the scheduled time was made by the participant or the researchers. The first part of the interview was dedicated to explaining in greater detail the scope of the research, its particularities, as well as addressing any questions that the participant might have. Following the formal introduction, the second part of the interview focused on obtaining a summary of the participant's background. This was done to get a better understanding of his professional path, as well as to gain insights as to why he might have certain opinions on the subject studied. The third section of the interview was dedicated to the field of cyber insurance and the participant's perceptions thereon. This section was at the core of the research and directly related to the research question; by it, we tried to get a better understanding of how cyber insurance is perceived by the interviewees. Additionally, the section was designed to look at the different tools, techniques and data used to draft a policy and use insurance as a tool for risk governance. Finally, the fourth section of the interview pertained to the participant's relationship with regulating bodies and third-party companies. Although there was a predetermined structure to the interview, it is important to note that these questions were not necessarily asked in succession. In fact, during the interactions, we allowed the participants to speak about their experiences and views freely. This was done to offer interviewees freedom in the information they wanted to provide, which is in line with Grounded Theory (Poupart, 1997). The structure, thus, was created to offer

only an initial guideline to the interview. However, it was rare that we had to bring a participant back to our structure; he would offer the answers to the structured questions without interruptions by the interviewer. This was beneficial as it allowed for a theoretical sensitivity, which consists of "placing preconceived ideas aside and immersing oneself in the data to discern what the participants perceive as meaningful" (Charmaz, 2012, p. 5). Thus, this allowed us, as interviewers, to construct our theory as the data was continuously received and analyzed (Charmaz, 2012). This process was also used when doing in-person interviews.

2.3. Data Analysis & Coding

While sequentially doing interviews, it is important to conduct a process called the constant comparative; such implies that the data emerging from interviews must continuously be compared and analyzed with previous interviews to look for similarities and differences (Walsh, Holton, Bailyn, Fernandez & Glaser, 2015). To do so, Grounded Theory implies that a standard approach divided in three specific categories must be applied. These categories, which aim to develop a substantive-level theory, are open coding, axial coding and selective coding (Creswell, 1998). Briefly, Bryant and Charmaz (2007) suggest that this process starts with open coding, which then gives way to the emergence of core categories, which are followed by a "delimiting of data collection and analysis for selective coding to theoretically saturate the core category and related categories" (275). Additionally, Creswell (1998) suggests that some research grounded in theory can create a visual portrayal of a conditional matrix, which will explain several phenomena, such as the social, historical and economic context that influenced the theory that was developed. That said, we abstained from further developing a conditional matrix as it was not used within this research.

The first constant comparative is the open coding, which consists in creating initial categories of the phenomenon that is being observed. Within these categories, the researcher must find several subcategories that will be essential to provide a dimension or show the different possibilities that the gathered data can form (Creswell, 1998). This first part can be considered a tentative approach to developing the theory. According to Strauss and Corbin (1998), during the early parts of open coding, the researcher must write different notes pertaining to his own personal thoughts, ideas, directions and impressions. By adopting this first step, the researcher will start asking himself relevant theoretical questions that will enable the emergence of initial categories (Strauss & Corbin, 1998).

To facilitate theoretical sensitivity, the interviews were recorded, which all the participants agreed to. Following the interview, the recordings were transcribed in Microsoft Word where the document was divided into three distinct parts to avoid getting lost in several pages of notes. This also facilitated the labelling of categories. There are several software, such as Mendeley, QDA Miner and Zotero, that facilitate the coding of the data. However, the coding was done manually with the use of colors and adhesive memo papers (Post-It) due to the habit of using such a method for previous research.

In regard to the labelling, the first part contained all of the interview written verbatim. The second part contained the summary of several passages that seemed at first glance to be relevant to the research question. Finally, the third section was reserved for different codes assigned to the passages that were of relevance. These codes served to form initial categories and subcategories of the data. This approach, as suggested by Paille and Mucchielli (2012), allowed us to identify similar key words and reoccurring patterns with other interviews.

Following the open coding, the axial coding was used to continue extracting data from the interviews. According to Strauss and Corbin (1998), axial coding is the process by which categories and subcategories are brought together and analyzed. This enables a better understanding of the categories and subcategories and allows one to combine them via a coding paradigm. According to Creswell (1998), the coding paradigm allows the researcher to conduct four specific tasks in order to be theoretically sensitive. These tasks are the following: Identifying the central phenomena conditions; Looking for causal conditions by which categories or subcategories can be found that will impact the phenomenon; Specifying strategies, which are the "actions or interactions that result from the central phenomenon" (Creswell, 1998, p. 57); Finding the context and the intervening conditions that will affect the strategies; and, finally, defining the consequences of the central phenomenon (Creswell, 1998). It is important to mention that this part of the analysis of our previous notes is the actual data. For Strauss and Corbin (1998), axial coding allows the researcher to develop different ways of analyzing the data and conducting further interviews. Additionally, it can help the researcher focus on certain categories or subcategories in future interview analyses (Strauss & Corbin, 1998).

With the framework established by the axial coding, we started to think analytically about the subject. In fact, we started exploring different definitions given of cybercrime and cyber insurance, and the role the latter plays in risk governance. In addition, we took various categories and subcategories and furthered their analysis. This was done to summarize certain information in order to answer the four categories of axial coding. To enable this process, we followed Strauss and Corbin's (1998) suggestion to create several diagrams, which allowed us to sort out the different relationships observed in our categories. Moreover, we used a separate box to create new categories that emerged within the data. This was done with the general understanding that, during

the early process of axial coding, some categories might be briefly defined or seem irrelevant altogether (Bryant & Charmaz, 2007). However, as Grounded Theory suggests, until the data saturation is achieved, we must keep going back to the field of study to explore and find new information. Hence, by creating a box with new categories, we were continuously reminded of other subjects that were worth exploring and that may eventually become relevant.

During the final part of our data analysis and coding, we followed the rules implemented by the selective coding. Selective coding is where the researcher integrates the findings elaborated in the axial coding. For Creswell (1998), this is where the researcher creates a story and where conditional propositions are presented. In fact, Strauss and Corbin (1998) claim that this is the final step of the analysis where "the integration of concepts around a core category and the filling in one of categories in need of further development and refinement" takes place (236-237). Generally, in this final category, fewer codes are found; however, there were more theoretical notes, which completed the final categories and, thus, elaborated the emerging theory. In fact, as we approached the end of the data analysis, our diagrams were used to elaborate our data whilst creating our theory (Strauss & Corbin, 1998). This was done by taking our descriptive categories and translating them into analytical ones.

As we neared the end of our coding and analysis, the selective coding helped us develop three important categories with several subcategories. To facilitate this process, we followed the indications of Strauss and Corbin (1998), namely, creating and bringing together the data found in our diagrams and memos. By applying open coding, axial coding and selective coding, we hoped to achieve a certain level of saturation suitable for answering our initial research question.

3. Methodological Limitations

Grounded Theory might seem like a research tool that allows the researcher a considerable amount of freedom. However, it is on the contrary an instrument that imposes rigorous procedures to be applied throughout the whole research process. Hence, these strict guidelines have contributed to certain limitations within the application of this methodological framework.

Our study did not follow the optional fourth principle of theoretical sampling, namely, theoretical group interviews (Bryant & Charmaz, 2007). Theoretical group interviews refer to the process by which we could have gathered a small group of the participants with whom we would have shared our initial findings. After doing so, the group would have discussed the findings and potentially offered additional insights that could have benefited the emerging theory (Bryant & Charmaz, 2007). However, only one interview was conducted with each participant. While we believe that more interviews with the participants could have added value to our data, many of these professionals did not have time to take part in such due to their demanding schedules. Our timeframe was also limited.

Another limitation associated with Grounded Theory has been highlighted by several researchers, such as Timmermans and Tavory, as well as Gibson; they have noted that, by employing this model, one cannot create theoretical sensitivity without any preconceived knowledge of the subject (Bryant & Charmaz, 2007). However, to circumvent this potential problem, our literature review was completed not with the intention of enhancing our understanding of the subject matter but, rather, with the goal of creating and guiding our initial selection process through theoretical sampling. Additionally, the literature is often concerned with how other authors and researchers understand cyber insurance and what their perspectives are on the matter, given that some studied the subject using preconceived theories.

In relation to the notion of preconceived knowledge, researchers such as Locke (1996) and Walsh (2015) believe several studies that claim to employ Grounded Theory do not fully grasp its premises nor how to apply it in a study. Both Locke (1996) and Walsh (2015) argue that the theory is cited but not fully applied by researchers. Rather, Locke (1996) and Walsh (2015) argue that people tend to use this method for the apparent freedom that it allows within a study. Yet, they omit applying strict rules imposed by the theory, such as the rules of theoretical sampling. For Walsh (2015), this leads researchers to create their own conceptual framework which harms the epistemological framework. Additionally, Suddaby (2006) believes that ignoring GT's recommendations can potentially harm the interpretive analysis of the data. The author believes that, instead of generating the theory through a strict analytical process, one will deduce results based on observations that are not separated from her preconceived ideas (Suddaby, 2006). Hence, to circumvent this potential problem, we opted to apply strictly the methods suggested by Strauss (1992). Strauss (1992) insists that we must continuously and conceptually describe all our observations. Using this form of analysis then allowed us to fully generate theories while limiting our preconceived notions that could have hampered the data being studied.

CHAPTER III: DATA PRESENTATION

The Grounded Theory developed by Glaser and Strauss (1967) was used to generate a theory for this thesis regarding how insurance companies conceptualize cyber risks to quantify a residual or evolving loss. Additionally, this rule provided a better understanding as to the role insurance plays as an alternative to risk governance. Following a thorough theoretical coding process, the data obtained through the interviews revealed that cyber insurance is a preventive tool that takes on the role of three predominant factors: Understanding Cybercrimes, Risk Management and Behaviors Towards Risk and Surveillance and Governance. These three factors contributed to form an alternative to traditional governance methods such as anti-viruses, firewalls and anti-spywares. This section will discuss our findings, as well as the theoretical concepts that look at how cyber insurance becomes a tool for risk management and governance.

1. Categorization

Throughout the coding procedures, each interviewed participant was given the opportunity to express their own personal understanding of cyber insurance. The participants in the research hold roles within the field of insurance that are all equally important. For example, the insurance broker must continuously stay in touch with underwriters to obtain policies and quotes for their clients. However, the participants did not always display similar points of view regarding cyber insurance. Of course, because of the relatively new presence of this product on the market, some experiences and views varied to a certain extent. Thus, several categories, which encompassed the meaning of cyber insurance from each participant, were created.

1.1. Cyber Insurance Defined

As cyber insurance is a new product in the market, insurance companies strive to understand and assign a definition to this new risk. This is done with the goal of offering a product that meets the coverage needs of their customers. The data obtained through interviews suggest that every company assigns a different meaning to what is covered by the insurance. Thus, understanding and defining cyber insurance and what it will cover is of greater importance, because the CGL has not viewed cyber losses as an insurance property (Yu, 2014). Moreover, for over 25 years, there was a computer crime policy that existed and according to participant 1, this product strictly covered the loss of funds. In fact, the main observation to make when defining what is covered by cyber insurance lies in understanding how the loss is incurred. The importance of the distinction made by these two types of coverage is based on the fact that many companies do not purchase cyber insurance. As seen in the Sony Corp. America vs. Zurich Re case, participant 4 states that companies that get breached will see if they are covered under the crime policy. Furthermore, traditional crime policies offer coverage for attacks made with the use of a computer. However, the difference between a traditional crime policy and cyber policy lies with how the data is acquired and what purpose it serves. As an example, participant 1 believes that:

> If the industry gets hit with a loss, one of the areas we see that is being questioned is whether the loss is a result of a direct hacking activity or a loss of data. Thus, this is a big issue to sort through to see where the loss resides. Is it in a crime policy or a cyber policy?

For participant 1, the loss of funds should reside with a crime policy, because it directly deals with funds as opposed to data information which is not considered a tangible asset. Data information is considered valuable, but it is not immediately monetized. Thus, if you can sell the data for money

then it is a cyber related loss, but if you purposely take money out of the system it is a crime related loss. Similarly, participant 4 offers the same understanding of what differentiates a crime policy from a cyber policy. He argues that:

> The commercial crime policy might say we [i.e., the insurance company] will pay losses sustained by the insured that are directly the result of computer fraud through a third party. Thus, if there is an unlawful taking of money using a computer system, it will be considered a crime policy (Participant 4).

An example to demonstrate what is a cyber insurance loss is given by participant 10. He explains that if there is a negligent employee that facilitates access to a computer system from a third party, and this results in money being taken out of the company's account, it will generally fall under a crime policy.

Based on the differences between a crime and cyber policy, it is evident that insurance companies try to define a cyber risk effectively in order to act as an additional tool to govern cyber risk. Based on several participants (1, 2, 8, 9), it seems that it is generally agreed that each company has their own particular definition of cyber insurance coverage which generally covers first party acts of online intrusions where information regarding the privacy and information of a company or an individual has been unlawfully accessed in a computer system through certain techniques like DDoS, Ransomwares and phishing tools. It also covers third party losses which are related to notification costs that companies must undertake to warn their clients that their information has been breached, as well as credit monitoring services. Third party losses also cover legal costs in the case of lawsuits, and public relation firms that help restore the company's public image.

1.2. Wording

When defining cyber coverage and offering adequate protection, just like any other policy, the wording of the policy plays an important role in order to determine if the breach is covered under one's cyber insurance. This is in part due to the evolving nature of cybercrime and the understanding that an insurance company has of the risk. According to participant 2 and 8:

> Security and privacy policies' coverage, just like technology, are continuously evolving. Therefore, we need to update our wording at least annually or rewrite policies by adding endorsements to comply or take into account the development of laws and technologies (Participant 2).
>
> Every insurance company updates their wording every now and then. In regard to cyber, its wording is being widely used with different meaning for individuals and companies. Thus, in the cyber world, it changes every two to three years. This is done to be in line with other companies and to keep a competitive presence in the market (Participant 8).

The wording of policies is not only a priority for insurance companies to be able to offer competitive products, as well as be relevant to the market. The wording also plays a significant role when the insured company and the insurer are facing legal battles in courts so as to determine if the breach is covered under a cyber policy or crime policy. In fact, it was suggested that many merchants do not favour the purchase of cyber insurance. Many factors can be attributed to the refusal to adhere to such a product. For one, participant 3 suggests that some cyber policies may cost more than a regular CGL insurance. Participant 1, moreover, describes cyber insurance as an added cost that is not worth the investment. This is due to the fact that many small to medium business owners believe that an attack will not target them, because they are not a large

conglomerate. Similarly, participants 2 and 5 have observed this thought process amongst larger companies. Often, Chief Executive Officers (CEO) or Chief Security Officers (CSO) analyze their security investment through a cost-benefit approach and deem the cyber protection too expensive. However, when these companies are faced with a breach, and realize the investment cost required to restore their business activities, they look for loopholes in policies they already own, such as the crime policy, the CGL or the Error and Omission (E&O) to see if they can be compensated. An example of this scenario is given by participant 4:

> The most important thing to keep in mind when looking at your cyber coverage is that it depends entirely on the policy wording and there is no standard wording yet. It depends on the wording of the policy on how cyber is determined. I've seen policies that had over 25 coverages and the first one might say we cover for any lawsuit against you in regard to a hacking incident. Then the question becomes, is this a hacking incident? And the policy will give a definition of hacking. So, the policy itself tells you what is covered and what isn't. This is because there are all kinds of cybercrimes and therefore there are different provisions, such as for ransomware. The courts will then see it as a contract between two parties and will make a decision based on how they interpret the meaning of the wording, on previous case laws and the opinion of an IT expert (Participant 4).

This concept of wording also seems to impact the work of insurance professionals. In regard to the broker's perspectives, every client has certain needs in terms of IT protection. Hence, as suggested by participants 5 and 10, a broker must evaluate the needs of their clients and look for the best coverage for their business. This is of greater importance because provinces are governed by regulatory codes. For instance, Quebec, according to participant 9, is controlled by

the *Regroupement des cabinets de courtage d'Assurance du Québec (RCCAQ)*. Therefore, it is important for the brokers to respect a deontology code which consists in conducting in-depth analyses of their clients' needs. However, as participant 5 suggests, no cyber policy has the same coverage wording. Cyber products differ among every company as they carry different limits, premiums and they all cover different things. This diversity seems to be, according to participant 5, the result of a lack of structure from regulatory bodies, such as the Insurance Bureau of Canada (IBC). Further, it suggests that the IBC gives a certain freedom for companies to develop their own coverage as the IBC is yet to develop a structure similar to the one seen with the CGL. As an example, participant 8 argues that:

> Cyber is very recent; 7 years is an infant in insurance. So, terminology is not common within all insurers. If you compare to other lines of business, such as the CGL, which goes back 200 years, everyone has a similar definition, as the IBC sets coverage standards and companies cannot offer less. From a cyber standpoint, the IBC did not set any standard, and most companies develop policies on their own; the terminology is not widely accepted by competing insurance firms. (Participant 8)

These limits become quite complex as brokers, according to participants 4 and 9, need to develop IT knowledge in order to better serve their clients and suggest which coverage might be better suited for them. Moreover, the brokers must also be cautious to avoid underinsuring their clients. Several companies have offered general cyber insurance coverages, but these products do not fit the requirements of the clients. As an example, participant 3 mentions:

> If I have a small client, I can add for $94 a basic cyber policy. If we sell a full cyber policy, Intact won't offer it and we need to go to an MGA who actually writes full blown cyber policies. This is because a $94 coverage is not enough as a breach can

> cost over 100 000 dollars just in notification costs and Intact will only give $25 000 which is not enough. Thus, that small package will result in clients being underinsured. (Participant 3)

However, this difficulty also affects the underwriters. As previously mentioned, cyber insurance can be quite expensive and each company will cover the risk in their own way without a predetermined standard. Hence, participant 8 mentions that, on several occasions, brokers have gotten back to them with cheaper quotes from other companies and ask if they can match the price. This appears to be a difficult task because he is not aware of the wording and the coverage offered by his competitor. Participant 8 offers a great example of this problem:

> It's always a bit challenging to compare ourselves to competitors and that is the challenge for brokers as they get quotes from different carriers and want to recommend to their client what is the best quote. So, obviously the premium is very important but it's like buying a car. If I offer to buy you a Lexus, a Honda or a Lada, the price will be very different. From a cyber perspective, it's very difficult for the brokers to compare the terminology used from one company to the next and factor the price difference. Similarly, for us underwriters, it's hard as brokers can say "I got a better quote from a competitor, can you match it?" Well I may offer a higher premium and have a better coverage but really how do I know if I have access to the competitor's wording. Yet my reading is only my interpretation and I am not in their shoes to understand what they are saying.

The wording plays a significant role in what the insurance will cover and how it can help govern the cyber risk. Yet, other factors were observed with the various interviews, and another main concept in regard to governance is deduction and cyber resiliency.

1.3. The Lack of Data

Throughout the literature, the absence of data has been often singled out as the main challenge that insurance companies must face when drafting a cyber policy. For participant 7, this is due to the limited number of claims that are made every month in Canada. Therefore, it is of interest to know what companies will do and how they will do it in order to push the sale of a cyber policy. Additionally, as it was presented in Category B, different policies have different wordings which can create a great deal of complication when selling the policy to customers. Hence, there is an evident relationship between the disparity of wording and the lack of data made available to the insurance companies. This can be observed in participant 1's statement:

> When it comes to the actual coverage itself, the industry has a pretty big blank on what is the quantification of a cyber breach policy. If the industry gets hit with a loss they did not foresee, that is when we will see the evolution of the product. (Participant 1)

Similarly, participant 2 mentions this problem:

> When we have the risk defined, we do our best with the actuaries and the product underwriters to analyze and quantify the different security and privacy risks. However, we need more data to be available because the data is not very robust. (Participant 2)

Despite the lack of data, insurance companies need to develop products in order to compete with their rivals and offer their clients viable options. Thus, when faced with a minimum amount of quantifiable data, participant 2 explains that his company uses a theory coverage to estimate the potential claim. This is done by analyzing the companies' infrastructures and data they hold, as well as previous claims that can possibly help them make an educated guess. However, as participant 5 notes, every cyber insurance policy is written differently and there is not a set method. Rather, he feels that insurance companies are just "throwing a dart" at what will be covered:

> They tend to look at what is going on, and it's kind of throwing a dart and saying, this company fits in this risk demographic; they have this revenue, security system and data; well, they will charge X dollar amount. (Participant 5)

Participant 8 also suggests that when quantifying the data, it becomes somewhat of a guessing game.

> This product is in infancy and everybody – brokers, insurers and insured – are all trying to figure it out. Obviously, if you are trying to insure the convenience store next door which does not even have a credit card payment system and has very little personal information, well the exposure is not so high; you can think that a million-dollar liability is sufficient. If you have a company like Target, and you want to offer higher limits in liability and 100 to 150 million in first party coverage, you draft a policy based on that information and sometimes your guess can be as good as mine (Participant 8).

However, it is important to mention that when analyzing a company that applies for cyber insurance, its revenue does not carry the same importance as the actual data it carries. As, an example, participant 5 explains that, even though one company makes an annual revenue of 100 million dollars and holds records and/or patents of their business activities, their information is not as vulnerable as a company that generates 10 million dollars in revenue but holds thousands of Social Insurance Numbers (SIN). To summarize how the policy will be drafted, participant 7 offers a brief understanding on how it is evaluated:

> For me, a lot of it comes from what you are doing, who are your customers, the data you have and what is your brand name (Participant 7).

Despite suggesting that, when drafting a policy, it becomes somewhat of a guessing game or a theoretical coverage, this technique is supported by a questionnaire that is required to be filled-out by the company requesting cyber coverage. For participant 3, this is required not only because there is not enough quantifiable information but also because every industry faces different realities and the information they hold can vary from one to another. Thus, the questionnaire allows the underwriter to get a better assessment of each company so he can better offer coverage. However, amongst many companies, the application may vary. For some it can be one page, while for others it can be a detailed questionnaire that goes well beyond 15 pages (Participant 3). Participant 3 explains the relevance of the application by stating the following:

> Everyone is underwritten according to an application that clients need to fill in. The one we deal with most is a one-page application, but some carriers ask for 15 pages and all the specifics. Some ask for one page because they know that the risk of getting hacked is high, so it does not matter what hardware is in place. All they ask is that the company does back-ups on a daily basis and has a firewall in place. Other carriers can require 15 pages to be completed, and can decline the application if the area is a high risk. (Participant 3)

An example of what is asked in a detailed application is given by participant 2: before they issue a particular coverage to their clients, they require the company to fill out an application which gives the underwriter a better understanding of the security standards and controls put in place. When assessing this application, the underwriter seeks to analyze different factors than can help prevent a cyber breach and in turn reduce risk. In general, this application will check that a company has the following measures; a comprehensive security plan in place, understanding where the data is stored, a minimum control system which includes firewalls, good password

control, good patch management, strong monitoring and intrusion detection controls. Additionally, they should have a viable continuity plan and incident response program in case their protection is breached (Participant 2). If these measures are not in place, there is a possibility that the company will tell their clients that they cannot protect them unless they do so. Nonetheless, participant 2 does mention that, even if a company does not have a strong security infrastructure, the insurer can issue them a policy if the underwriter judges that the risk is not too high.

Although the application is a viable tool to get a better understanding of what needs to be insured, some do not see the pertinence of sending it to clients. Participant 7, for example, argues that most of these questions are simply yes or no answers to standard security measures. An example of these questions can be: do you have an anti-virus? Do you have a firewall? Do you have physical security, etc. Participant 7, further, believes that originally these questions were simply designed to "prevent the low hanging fruit," meaning, to deter companies that do not put anything in place to protect themselves from a breach. However, these questions do not seem as relevant because you can get breached regardless of the security measures in place. A breach can occur simply because an employee wrote his email under his keyboard or the employee did not take precautionary measures when opening a phishing email. Thus, a new questionnaire should put a greater emphasis on risk response processes put in place by the company to ensure business continuity. Additionally, questions should be geared towards asking if there is training offered to employees regarding cyber security, if there are security plans updated every 6 months, or if the company has best practices. Such questions will allow the underwriters to see if the company will be able to get back on their feet and restore their operation while reducing their downtime and limit the damages inflicted by an attack.

The lack of data regarding cyber insurance in Canada evidently requires underwriters to use their instincts, in conjunction with the application, for the drafting of a policy. Nonetheless, there is also another tool at their disposal which is looking at how Americans draft policies. As it was previously mentioned, the U.S.A. has put in place legal provisions that require companies to disclose when a breach occurs, thus creating a higher number of claims to their insurance providers (Yu, 2014). As a result, Canadian insurance professionals can consult claims and strategies made across the border.

Participant 3 claims that the U.S.A has started writing cyber insurance policies for about 10 years now as opposed to the Canadian landscape. Thus, she contacted a Managing General Agent (MGA) in the U.S.A. to place the cyber risk with the U.S company as they specialized in writing unconventional policies. Like participant 3, participant 7 also used the same approach:

> Four years ago, a standalone cyber insurance product launched and when it came out, I worked with a U.S company. The U.S. laws are more robust which allows for more information gathering and the creating of more comprehensive cyber coverages (Participant 7).

The importance of looking at the American legal system and claims also lies in the Canadian courts' lack of knowledge in properly judging court cases regarding cyber breaches. Several participants, such as 7, 8 and 10 argued that, while the laws forcing the disclosure of breaches will come about in the near future, as there are advanced talks regarding the Digital Privacy Act (2015), Canadian courts are unable to fully render a decision in these cases. Participant 7 believes that lawyers are not interested in these lawsuits because they take a lot of resources; they also feel that a big class action lawsuit will take several years to litigate in the courts and the money involved might not be worth it. Additionally, participant 4 argues that Canadian judges do not possess the

necessary knowledge in making decisions in these cases and will often rely on what has been decided in American contexts. Moreover, because there is uncertainty as to what is considered insurable, most cases, about 80%, will be settled outside the courts. This leaves the insurance companies with a minimal amount of information regarding cyber policies, and how and what should be included under such coverage (Participant 3).

1.4. Information Networks

Building on the information presented in the previous section, it seems that insurance has struggled to find adequate data to develop viable cyber coverage. A main category that came up in the interviews was information sharing. It is common knowledge that, in order to develop policies, you must have quantifiable data. Likewise, by quantifying data corresponding to data breaches, insurance companies can create products that are much more resilient and will contribute to the governance of the cyber threat (Participant 9). Hence, developing information sharing networks seems to be an important preoccupation for insurance professionals; it will allow them not only to perfect their products, but also to facilitate sales as clients will be much more aware of the threat and the premiums will not be as excessive. To optimize information sharing, the participants suggested that it should be done at three distinctive levels; government bodies, companies and insurance professionals.

1.4.1. Government Bodies

One of the main distinctions that differentiates American and Canadian cyber insurance markets is the legislation enacted by the American government, which requires any company that is breached to render that information public (Insurance Institute, 2015). This, according to participant 7, allowed for better cyber insurance coverage to be available to the public. However,

because Canada has yet to pass the Digital Privacy Act (2015), companies are not obliged to release this information publicly. Therefore, cyber policies in Canada have not been as valuable for business owners as they have been for their American counterparts.

For participant 5, the cost of cyber insurance is the main barrier and reason why it is not a product purchased by a majority of business owners. He argues the following:

> The cost of cyber insurance is the biggest entry barrier and until there is a requirement for you to notify people of a breach, until that point it will be an expensive product that some may or may not purchase.

According to participants 9 and 10, forcing the notification of a breach will not only generate more data for insurance companies and consequently drop the prices of policies, but companies will voluntarily enhance their IT security systems, which will then reduce the possibility of considerable damages due to an attack, and result in reduced insurance prices.

Although the Canadian federal government has yet to enact the Digital Privacy Act (2015), there are some provinces that enacted provisions that force certain breaches to be brought to light. As an example, participant 3 mentions that in Alberta and British Columbia, laws are somewhat more restrictive in this regard. In fact, when a breach occurs, the commissioners of the respective provinces will evaluate how serious it is and can possibly require the targeted company to render that information public (Participant 3). Similar approaches are also observed in the Quebec and Ontario provinces, although therein laws are limited based on the nature of the information accessed. Both participant 5 and 8 argue that, if such measures are taken by the provincial governments, it is usually pertaining to information related to the medical field or, like in Ontario, the records of 500 000 students that were breached. Despite that most of the study participants are in favour of the Digital Privacy Act (2015) as it will give more data to insurance companies to

work with, participant 6 does not believe that it will be the case. The participant argues the following:

> The S-4 Bill[1] will simply update the PIPEDA Act. It does not change much as with or without that legislation on this issue, there is not enough case law and history that will dictate this type of claim. You do not need statutes to force companies to come clean as it's good practice… if you don't you will expose yourself to more litigation. If you come clean, you can show the court that you acted in good faith. Therefore, I do not think that the legislation amendments will change anything especially in insurance (Participant 6).

That being said, participant 10 argues that, on the contrary, when the government will force companies to divulge the breach it will be of greater impact for the industry as a whole. The participant believes that insurance is like a pool of water and one drop will not make a difference. However, if everyone comes together and the government obliges notifications of cyber breaches, this will allow for more quantifiable data, reductions in the cost of policies and stronger security infrastructures for companies.

1.4.2. Companies

Governmental policies will play a big role in helping the development of cyber insurance. Nonetheless, insurance professionals have also called upon companies to contribute to this effort. The effort, however, does not only come from those who have been breached, but also from companies offering additional security measures.

Participant 9 argues that the development of cyber insurance is significantly dependent on the companies that have been breached, though. Despite the possibility of laws being enacted to

[1] The Bill S-4 now became the Digital Privacy Act (2015).

force the disclosure of a breach, some business owners may choose not to disclose. According to participant 9, this can occur when the company fears facing class action lawsuits that can amount to millions of dollars, or simply because a cyber attack, unlike a fire, is not visible to their clients. This refusal to notify the public of the breach does not always play in their favour, though. For participant 6, if caught, the company will face additional lawsuits, such as professional misconduct, because they did not act in good faith. Moreover, participant 9 argues that by notifying the public of a breach it will not only allow the company to enhance their security software. It will also contribute to the reduction of the premium as the insurance company has more data to understand the risk they are facing. This opinion is also shared by participant 5; as mentioned in the preceding categories, the biggest barrier in the insurance industry is the cost of the policy. However, with more data obtained from companies, not only will the cost of the premium be reduced but it will also contribute to the development of much more comprehensive policies.

Other than requiring the company to share information when they are breached, it is important for companies to fully disclose what type of information they have and from where it is coming. This is significant because, as participants 4 and 8 explain, when a Canadian company gets breached and they hold information of Americans it is the American legal system that can prevail. The participants state the following:

> Right now, if a Canadian company has personal information of Americans, it's the American law that will apply. As an example, if you are a Montreal based company and you have clients in Quebec, Ontario, Alberta, New York and California and your servers get hacked, the lawsuits will abide from each of the provinces' or states' jurisdictions. For me, it is more important to know where the clients are instead of the servers (Participant 8).

> Depending on the case, they have a choice where to sue, such as the U.S.A or Canada. In the U.S. the laws are broad, so if you are a Canadian company and doing business in the U.S. you are potentially subject to the jurisdiction of the American courts (Participant 4).

With this being the case, participant 4 argues that it is important for an underwriter to know this type of information for a given company, because when he is writing the policy, he will take it into consideration. This will work in favour of the client as he can benefit from coverage that goes well beyond the Canadian border. In fact, participant 8 suggests that, despite the rate being much higher if you have information in the United States, it is to the client's advantage to disclose that information. This will allow him to benefit from a policy that covers breaches that involve the information of American citizens.

Additionally, partnerships with firms that provide additional security must be undertaken. In the following section, we will go in depth into how these companies, along with insurance, can contribute to a greater network resiliency. In particular, we will look at the benefits for such partnerships. According to participant 1, there are several firms that are used to monitor, identify and find solutions to enhance cyber security for their clients. Hence, participant 1 believes that information sharing with these security firms can be quite beneficial; it can contribute to and expand the quantitative information on cyber risk. He states:

> I think their data can be sold in terms of reports, and I think it's one area where insurance can go as it will buy their data and it will be helpful to analyze and quantify, which will then help them [i.e., insurance clients] with their protection and loss (Participant 1).

However, this idea is not shared by participant 10. He believes that when companies make a claim to their insurance, the insurance company will automatically have access to the data. Therefore, the data that these IT securities offer is not necessary. He sees them rather as a mandatory service that clients must purchase to reduce their exposure to the risk.

1.4.3. Insurance Professionals

A third means to facilitate information sharing is through insurance brokers. For participant 9, insurance brokers must act as the middlemen between their clients and the underwriters. The brokers must help their clients realize the data they have in their possession and who may want it (Participants 5 & 9). This is of great importance, because people do not seem to understand the information they hold nor, therefore, the risks involved. Participant 9 gives a pertinent example of how cyber insurance can apply to several industries whose management may not realize it. He uses the example of a fruit importer and states that, if you import fruits, you do not have any client information, but you do have a list of the inventory you are expecting online. If you get breached, you lose all of that information and are not able to keep track of your product coming in. This basic example shows how insurance professionals need to develop cyber insurance through different deduction techniques and promotion of the product. By doing so, according to several participants (3, 5, 7, 8, 9), if the clients understand the potential financial losses that a breach can create, many more business owners will purchase cyber coverage. Thus, if there is more risk, it will lead to a greater number of claims and in turn a greater public knowledge and quantitative data. Of course, as we saw in the previous sections, despite understanding or being aware of these breaches, business owners might not be interested in purchasing these protection products as they are expensive. However, participant 8 argues that, with more claims and a better understanding of the risk, the premiums will potentially be reduced.

1.5. Cyber Resiliency

To apply for cyber insurance, as previously mentioned, a company must fill in an application which will give a better understanding to the insurer of what needs to be covered and under what policy. Additionally, insurance companies also offer their clients other services that can enhance the companies' own network security. Thus, through the cyber resiliency category, it seems that insurance companies act as middlemen between companies seeking cyber protection and companies dedicated to providing it.

According to participant 1, his company can offer their clients a support system that can enhance their cyber security. As an example of what can be done, participant 1 mentions the following:

> We basically help companies get anywhere they are at to a safer side of things. We can help support the response planning of the organization and form a seamless risk management approach. (Participant 1)

Participant 1 also contracts third party firms that will do an assessment of the companies' security systems. They, further, offer services that include monitoring capabilities and breach identification. This is done not with the intent of enhancing the cyber security of the company but to get the posture of the organization in terms of security. Additionally, participant 1 believes that the majority of companies, particularly small to medium businesses (SMB), do not have in-house experts that can guarantee the security of their network. Participant 5 argues that this is a significant problem as SMBs carry a lot of significant data and do not want to purchase cyber insurance due to the elevated cost. Thus, by asking the insurance companies to conduct such assessments or hire third parties to monitor the cyber security aspect, this can be beneficial; it reduces the chances of a breach occurring and possibly premiums for the coverage, making the purchase of such more

attractive (Participant 1). However, there are strong possibilities that the client will, nonetheless, refuse the policies. In such a scenario, participant 5 believes that the only remaining benefit is that they educated the business owners of the reality of a cyber breach.

Similar to participant 1, participant 2 mentions that his teams of insurance professionals get together in order to look at what the best practices are for privacy controls and try to figure out what controls companies should have in place to safely guard their data. Moreover, participant 2 states that his company does have inside experts that can conduct the same functions as mentioned by participant 1. He believes that this is of great importance, because often organizations are not aware of the data they actually have and even if they are, they are unable to understand their own risk. Thus, by having the inside expertise, insurance companies can help companies adopt stronger cyber security practices. Yet, it is important to mention that not all insurance companies put so much effort into understanding the cyber threats to an organization. According to participant 3, certain insurance companies believe that every company can get hacked. Therefore, it does not matter what hardware is in place; such insurance firms are not actively trying to determine the actual security background of companies.

Other than offering cyber security assessments, participant 3 argues that cyber policies also offer the possibility of facilitating a fast response time following an attack. In fact, she argues that it is necessary to contact these security firms provided by insurance companies as they are properly trained to diminish the risk and find alternative solutions to solve a breach. Participant 3 states the following:

> Cyber policies are different. As an example, there is a 1-800 number for cyber policies. So, if you think you've been hacked, you call this number and they will place their own teams in the situation depending on the breach. If it was a ransomware that asks

> for $50 000 before the information is released, the 1-800 team will takeover to see if they can get that information without paying the ransom. It is really important that these people are contacted right away so they can help the client through the process. If the client tries to do it on their own, they will mess it up 9 times out of 10 as their IT guys are not appropriately trained like the company that will help them get through.

Just as the response teams are necessary to assist organizations that have been breached, insurance companies also have IT experts that will analyze the breach. Of course, this is done to investigate the claim and ensure it is not fraud against the insurance company, but according to participant 6, this also helps the breached company to understand what happened and how a cyber attack can be prevented. In terms of how the breached companies will investigate claims pertaining to cyber attacks, participant 6 explains that it will allow the breached company to hire IT experts to investigate the breach and look for solutions to protect the network from future claims. It is also possible that bigger companies will have their own experts. If such a scenario presents itself, the insurance company will also bring in their own experts to verify the incident. However, not all business owners can benefit from this type of service if they did not purchase the right policy, or if they just purchased the basic packages mentioned previously. Nonetheless, participant 6 suggests that he would not necessarily ignore a request from such a breached organization. He would still recommend certain companies that can help with incident responses, but it would be paid for by the company that is breached not the insurance.

Similar to what participant 6 mentioned, participant 7 also argues for the benefits of holding a cyber insurance policy. He strongly recommends that businesses invest in cyber security or, if you are a SMB, to hire an IT security company. That said, the participant mentions that IT security companies create a false sense of security as they do not offer 100% protection, nor do they offer

contingency plans to keep the business running. Additionally, they do not offer business interruption services, such as those addressing public relation issues, legal counselling or notifications costs. Thus, it is to a company's benefit to have cyber coverage; if they do, the insurance company will help the business recover from second and third-party issues caused by an attack, services not given by an IT company. Finally, several participants suggest that, despite having strong IT security and cyber coverage, most companies absolutely need to invest in training their employees. In regard to cyber attacks, employees are often the main causes. Thus, by having a properly trained workforce, the chances of an attack can be more easily reduced (Participant 3, 5, 7 & 8).

CHAPTER IV: DATA ANALYSIS

Risk is something that needs to be accepted, challenged, eliminated or when possible mitigated (Elliot, 1960). The literature shows that insurance is not only a risk management service that eliminates or reduces the cost of a certain type of risk (Mowbray & al., 1979). Insurance, represents an institution of applied knowledge and social necessity. Moreover, insurers approach to manage risk allows them to have a considerable impact on the development of preventive measures, compensation for losses and the possibilities to engage in risk taking practices (Ericson & al., 2003). Additionally, information that is gathered by the insurance industry contributes to transformation of a hazard to a risk. This risk can be, to a certain extent, controlled. As Ewald (1991) mentioned, objectifying the risk will render it a normality. This permits organizations to better adapt their security measures and conceivably diminish their chances of submitting a claim (Heimer, 2003). This, however, also permits the insurance industry to govern and regulate the behaviors of risk takers, which in this case are privately owned companies (Baker, 2003; Heimer, 2003).

These social implications are made possible due to actuarial technologies and the concept of probability. Probability, according to Landsman and Sherris (2001), is determined by statistical data, economic expectations and fluctuations, as well as losses previously claimed on similar coverages. Although the concept of probability is present, according to our data, when a cyber policy is evaluated, cyber insurance products cannot rely on traditional actuarial models to issue coverage and a premium to a business owner. This discovery was facilitated using the Grounded Theory. In fact, this theory was used to deduce how insurance companies conceptualize cyber risks in order to quantify a residual or evolving loss. The results of this research did not lead us to a clear understanding of how the insurance industry conceptualizes cybercrime. Nevertheless, it

allowed us to find relevant concepts on the cyber insurance industry, particularly how new forms of risk are integrated in the field. This study also allowed us to discover how active players within the insurance field can utilize cyber insurance as an additional security tool to protect a company's virtual data. Based on the Grounded Theory, it is possible for the researcher to start with a research question, but through its methodological applications, develop and conclude different results (Creswell, 1998).

The insurance industry can act as a preventive tool in two ways. First, cyber insurance can only be considered a preventive tool if coverage is being considered by a company. By this we mean that business owners consider or purchase cyber coverage in respect to their cyber needs, such as the security of virtual data and its infrastructures. On the other hand, insurance companies, through risk classification, are excluding individuals deemed risky from their pools (Heimer, 2003). Second, it can be argued that insurance is a valuable preventive tool only if the applicants fall within acceptable risk categories. Due to the novelty of cyber insurance products, it continues to foster the same sociological implications that traditional products offer. This section highlights how cyber insurance not only acts as a financial preventive tool. Rather, this study reveals how its functions are one of many approaches to manage modern risk. These implications contribute to the development of preventive measures, compensations for losses, social planning and the freedom to take risks (Ericson and Doyle, 2004). These premises will be discussed through the following three sections: Understanding Cybercrimes, Risk Management and Behavior Towards Risk and Surveillance and Governance.

1. Understanding Cybercrimes

Ericson and his associates (2003) suggest that insurance institutions are effective risk managers that prevent the spreading of the risk. This is achieved by assign themselves the responsibility of quantifying and commodifying the risk through actuarial and underwriting practices. In turn, this facilitates the implementation of preventive measures and the indemnification of their clients (Ewald, 1991). To do so, insurance professionals will objectify anything that can be perceived as risk. These professionals, such as actuaries and underwriters, create policies based on a measurement of available data (Vaughan & Vaughan, 2003). This refers to the concept of ratemaking and probability. To measure data and create a policy, actuaries will analyze the risk based on industry statistics, a company's previous losses, and the insurance industry's accumulated data based on past claims (Rejda, 2011). To control the risk, insurer will typically call upon different actuarial models to predict the risk. Examples include the Monopolistic Cyber Risk Probability, suggested by Landsman and Sherris (2001), and the Utility Based Preferential Pricing (UBPP), suggested by Mukhopadhyay and his colleagues (2013). In turn, this renders the risk a normality and society will simply view the event as accidental (Ericson & al., 2003). As an example, car accidents are now associated as one of many risks that can possibly arise when taking the decision to enter a vehicle. However, cyberattacks are yet to be considered "normal". The data found that insurers are struggling to fully grasp this reality. Part of the issues, as stated by several participants (4-5-8-10), is that each company has different wording when insuring cyber. This is the also the case for regulatory bodies such as the IBC. Participant 8 mentioned that regulatory bodies did not implement specific guidelines when insuring against cybercrimes. Similarly, participant 4 and 9 mentioned that there is an urgency for the industry to

get a better understanding of IT knowledge as it will enable them to better asses their clients' cyber insurance needs.

To better understand the risk, it was reported that the insurance industry calls for the latest technologies. (Ericson & al., 2003). However, this does not seem to currently be the case for the cyber industry. To evaluate the risk, the insurance companies require business owners to complete an application that details the network security efforts made by the applicant. This application would allow the insurance company to classify the organization and evaluate the risk they face when cybercrimes occur (Majuca & al., 2006). This approach seems to reflect the concept of a Risk Management Audit (Vaughan & Vaughan, 2003) which is an in-depth analysis of a company's risk profile. Following the reception of this application, participant 2 explained that they will do an assessment of the needs and come up with a theoretical coverage. At first, this form seems to bypass the lack of data needed to establish insurance policies as it collects primary data that is not normally found in basic actuarial concepts. On one hand, it is a useful technique to contribute to the understanding and dissemination of knowledge about risk. Knowledge diffusion refers to "the spread of knowledge from an original source or sources to one or more recipients" (Robertson & Jacobson, 2011, p. 1). Robertson and Jacobson (2011) argue that knowledge diffusion regarding new technology is essential as it allows for innovation, implementation and economic growth. My analysis argues that knowledge diffusion is beneficial to insurance companies in two ways. The first is that by constantly reworking their wording and collecting information (data) regarding cyber breaches, insurance companies are turning a risk into a normality. This is made possible as insurance professional are continuously gathering a considerable amount of data, which will enable them to better predict the cyber risk. Despite the benefits of the application form, I also note that insurers are maintaining the concept of risk

classification. This is clearly highlighted when participant 7 mentions that most of these questions are asked to "prevent the low hanging fruit". It can be reasoned that insurance institutions are defining what are considered good cyber security practices and those that harm the risk pool. This, as it was stated in the literature review, is done to diminish the chances of a claim being submitted and leave the insurance institution with less funds for their investment portfolio (Heimer, 2003). After administering the audit, some professionals revealed that, to a certain extent, they guess what needs to be insured. For example, participant 8 explained that "you draft a policy based on that information and sometimes your guess can be as good as mine". Similarly, participant 5 refers to underwriting a cyber insurance policy as "throwing a dart" and hoping that the company will reflect the demographic they are insuring. From this feedback, I take away that risk classification, combined with this guessing approach, enhance the opportunity for crimes to be committed. In the event of a cyber intrusion, the company may not receive the necessary financial support to restore its cyber infrastructure to continue its business activities. Besides restoring business activities, field studies have shown that various consequences are associated to an attack. For example, there have been events where attackers accessed a company's clients banking information, social insurance numbers, medical records and other private information (Verizon, 2018). This, according to the Insurance Institute (2015), can eventually force companies to face several lawsuits requiring them to financially indemnify their clients and pay for credit monitoring services. Additionally, the breached company will need to change, update or restore its infrastructures. However, if a company does not have the financial strength to restore its business activities, it may completely cease to exist. In addition, I predict that it can increase the number of cyber attacks. As companies are not equipped to improve their cyber security infrastructures, I expect that a signal of opportunity will be received by attackers, which could facilitate opportunities for future violations.

Despite these limitations, I remain convinced that insurance can potentially develop sufficient knowledge about cybercrime and can become a significant risk management product. In the next section, we will examine the different ways in which insurance is adopted as a prevention tool.

2. Risk Management and Behavior Towards Risk

So far, we have seen that cyber insurance professionals have a limited understanding of cyber crime which forces them to guess their clients' coverage. This could create opportunities for crime because companies do not have the necessary financial support to strengthen their security measures, allowing hackers greater facility to access a company's data. This difficulty can be associated to the limited amount of knowledge and understanding that the insurer owns. Independent from the limits discussed, I noted that the industry is at an immature state yet forward-looking; it is taking steps towards cyber risk management. This reinforces Hacking's (1990) argument that the insurance industry is an institution that provides an understanding of risk while developing its science. In addition, it also reinforces the idea that insurance is becoming a social necessity since it has societal implications for a company's decision regarding loss prevention measures, social planning and freedom to take risks (Ericson & al., 2003).

The application method discussed in the previous section seems to be the preferred assessment model of insurance professionals. I deduce that using such an approach helps explain why coverages vary amongst companies. According to our category Wording and Lack of Data, insurance professionals use an educated guess. Therefore, the coverage fully depends on the actuary or underwriter's intuition-laden analysis. Consequently, this creates a struggle for brokers to find which coverage better suits the needs of their clients as different companies have different meanings assigned to the cyber coverage (Participant 2 & 8). Similarly, underwriters also struggle

to offer a coverage that matches the rate of its competitors as they are not aware of what was considered in other policies (Participant 8). Despite the differences found in cyber policies, the use of applications and theoretical assumptions leads to a considerable amount of effort being put into updating the wording of a policy and in turn implementing itself as a social necessity which enable business owners to take decisions on risk. As an example, participants 2 and 8, suggest that updating the wording of a cyber policy is done annually in order to stay competitive within the market and adapt to new realities.

I argue that continued efforts to make policies more comprehensible will eventually transfer knowledge to the insurance consumers. This can increase profits, but it also assists all applicants in making informed decisions. For example, participant 5 mentioned that those who do not adhere to cyber insurance policies will, at the very least, be educated of the realities of cyber breaches. This form of education diminishes the number of individuals that will take decision towards risk based on perception rather than the understanding of risk probabilities (Ericson & al., 2003). With knowledge transfer, an organization is better suited to understand the security gaps and take necessary steps to protect the data it holds. For example, the company may decide to improve its security measures and educate its own employees to adapt safer practices on the Internet. Verizon (2018) reported that a considerable number of attacks against a company are often facilitated by an employee's lack of awareness. However, if employees are better informed about this, it can reduce the risk of a company being the victim of a privacy breach. This supports Ericson and Doyle's (2003) argument that it ought to become a reflexive knowledge.

In addition to risk education, the insurance industry contributes to risk management through its audits. Generally, the risk manager, according to Vaughan and Vaughan (2003), must follow the following five steps; determine security objectives, identify the risks, evaluate the risks,

consider and select risk management products, implement security efforts and finally, evaluate the effectiveness of security efforts. Similarly, the Insurance Institute (2015) suggests that a company should apply the OSFI guidelines to establish an effective security framework. Based on the outlined tasks, I believe that insurance companies, when studying the insurability of a company, apply the measures outlined by Vaughan and Vaughan (2003) and the Insurance Institute (2015)

When looking at cyber security coverage, it was made clear that clients are handed out an application (participants 2, 3, 7, 8). I argued that this application allows both the underwriter and the applicant get a better understanding of the security framework that is present within his company and the value of the data. I argue that the 15-page application is better suited for the insurance industry if it were to successfully act as a risk manager. An advantage of the fifteen-page application is that a one-page does not serve and fulfil the role of a risk manager. This is deduced because participant 3 mentions that a one-page application is just to get a general understanding and that it does not matter what measures are in place; the probability of getting hacked is high regardless. On the other hand, by completing a detailed questionnaire, the insurance company will be better suited to fully assess their insurability (Participant 3). By doing so, as participants 5 and 10 mentioned, the insurance professionals will be better equipped to evaluate the needs of their clients. In turn, they allow for the implementation of an IRM plan, which is similar to participant 1's suggestion that his company supports the planning of a risk management approach.

An IRM plans usually consists of 4 mandatory steps, which are risk identification, risk analysis, risk reduction measures and risk monitoring (Bandyopadhyay, Mykytyn & Mykytyn, 1999). The first is to identify the risk. In this sense, the evaluation will conduct an analysis of a company's security plan, understanding where the data is stored, as well as the control system,

patch management, monitoring and intrusion detection controls that are put in place. In addition to these standard questions, I agree with participant 7 who mentions that the analysis must consist in verifying if the company has security plans, if training is offered to their employees and if the company has contingency plans set in case of a breach. It is also important to mention that not all companies face the same risk. As an example, participant 9 mentions that a fruit importer may believe that, because he does not own any client information, hackers will not be interested in his data. However, an attacker could hijack the shipment information and the vendor would not be able to deliver the products to his clients. Thus, this type of analysis allows the IRM plan to be customized to the needs of their clients.

The second step is to analyze the risk. This analysis is used to evaluate the extent of damages and losses that could be caused by an attack to an IT network (Bandyopadhyay & al. 1999). The interviews show that insurance contributes to this analysis by helping realize the nature of each company. In fact, participant 5 gives a relevant example as to how this is analyzed. He argues that it does not necessarily mean that because you have a higher revenue that cyber insurance will cost you more. A company that makes 10 million dollars in revenue, for instance, but holds thousands of SIN numbers is a lot more at risk than a company that makes 100 million dollars in revenue but only holds the company's patents (Participant 5). Thus, by keeping in mind the realties that any line of business holds, insurance companies can better inform companies about the potential risk they may face.

The third step of implementing an IRM plan is to adopt risk-reducing measures. As the questions in the application look at the security measures that are put in place, insurance can suggest additional security. As an example, participant 2 mentions that he and other insurance professionals will get together to analyze the security infrastructure of a company and will

determine if the applicant can benefit from coverage. However, if they judge that the client's security measures are not sufficient they may require them to enhance them to be insured. I believe that the first two steps will permit business owners to get a better understanding of what is at stake. Thus, as participant 1 suggested, they are potentially more likely to enhance their security measures if the risk is brought to their attention. Additionally, participant 2 mentioned that if additional security measures are adopted, an applicant can benefit from a reduction of the premium, and, if they refuse, they will not always be covered. Hence, due to the considerable financial impact of a cyber breach and the incentives offered by insurance companies, business owners will be more inclined to adopt stronger security measures.

The final step in the IRM plan is insurance helping companies with their risk monitoring. According to Bandyopadhyay (1999) and his colleagues, risk monitoring is the step whereby a company ensures that the security measures that are in place will continuously be implemented and strengthened if needed. However, this part will be studied further when looking at how insurance contributes to the surveillance and governance of risk as suggested by Ericson and his colleagues (2003).

Arguably, these steps persist in classifying their customers and do not make insurance a valid solution for some companies seeking to improve or invest in cyber security efforts. This seems evident as this application is used for the insurance industry to look for clients that are already cyber responsible and will not affect the integrity of the pool (Heimer, 2003). In fact, participant 2 clearly mentioned that clients can be refused coverage if they do not meet certain protection standards, unless they prove to enhance their security measures. I argue that the industry can also apply this concept to stay competitive within the market. The previous sections showed that different coverage is developed by the industry and they all differ amongst each other. In

addition, coverage can also be more expensive than the CGL. Thus, by pooling their clients and contributing to the risk classification, they will be better suited to offer a coverage with a price tag that entices business owners (Baker, 2003). Additionally, Baker (2003) also mentions that this enables the company to possibly transfer clients with a higher risk to their competitors.

Despite the evident goal of these risk audits from the insurer, it can however, continue to play a valuable role in the protection of cyber crimes. For one, classification is a collective sharing of burdens that creates a collective responsibility towards risk (Ericson & al., 2003). Similarly, Baker (2003), mentions that risk classification is a good thing as without it, low risk individuals would have to subsidize the high risks individuals. It also promotes both individual responsibility and the prevention of loss.

Of course, the decisions to purchase a cyber coverage are easily influenced by the cost-benefit analysis. Looking at security through an economic lens will facilitate the allocation of resources. Similarly, engaging in a cost-benefit analysis is done when a business owner looks at the data he owns, the probability of being attacked and the economic losses that can be suffered by his company (Gordon & al., 2003). Through the interviews, I found similar results. According to participants 3 and 5, many business owners are interested in cyber coverage. However, one of the greatest barriers to this product is the cost associated to it. For participant 3, the cost of cyber coverage can be more expensive than a regular CGL coverage. Additionally, participant 1 mentions that after seeing the price of a cyber policy, many business owners will not purchase the coverage, because it is too expensive, and they believe that an attack will not target them as their information is not valuable. Yet, I previously highlighted that over half of the breaches reported (58%) targeted small to medium businesses (Verizon, 2018).

This cost-benefit is a considerable factor in purchasing cyber insurance and security measures. Business owners may decide to continue with their current security measures. Regarding crime, this can have devasting effects. Evidentially, weak security measures will facilitate the opportunity of being attacked. In fact, this is shown through the Rational Choice Theory. The theory supports that individuals will engage in criminal behaviour if there is a given opportunity that will outweigh the costs (Kemshall, 2006). By neglecting preventive security measures, cyber criminals will view this as an opportunity to access sensitive information. However, it is important to note that the insurer's role as risk manager is only effective for those who choose and are chosen to contribute to the risk pool. Furthermore, the insurance only applies to cybercrimes for those who are considered insurable. An analysis for those that are considered uninsurable will be presented in the Surveillance and Governance section.

Though the cost-benefit ratio is a significant factor that can prevent companies from adhering to the implementation of security tools, I argue that companies who adhere to cybersecurity standards, contribute to a safer cybersecurity landscape. In this sense, these applications may be comparable to criminogenic risk assessment tools that seek to quantify data, in an effort to prevent crime or the risk of recidivism. That said, one can argue that these applications can only be beneficial for those who decide to buy a policy. I argue that this is not necessarily the case. The purpose of the audit is to assess a client's insurability. Although a client may refuse insurance, the audit identified vulnerabilities in their cyber infrastructure. In light of this information, the client may decide to implement security measures due to the absence of an insurance policy.

3. Surveillance & Governance

Undoubtedly, the complexities of cybercrime make it difficult to govern. The literature review pointed out that government agencies do not facilitate the development of cyber insurance in Canada. This is because mandatory notification laws are still waiting to be enacted (Shackleford, 2012; Insurance Institute, 2015). Yet, insurance can also help the government develop cyber security knowledge and practices. For Moss (2002), in Ericson and Doyle (2004), the State is at the head of risk management. Similarly, Garland (2003) suggest that in our society, governments are expected to act as the general risk manager.

Typically, the state is an information resource and communication hub for traditional crimes (Baker & al., 2003). However, regarding cybercrime, the governments and their law enforcement agencies do not possess all the knowledge and the financial power to deter and investigate the majority of breaches. (Choo, 2011). Through this study, I found that insurance is also information rich, and I argue that it should be a supplement to the governance of cyber risk. One of the reasons for this is that cybercrimes have no borders. For Choo (2011), there are not enough policing resources to trace a cyber attack. This makes public entities simply one of the many players that will contribute to a stronger cyber security environment. This view is reinforced by Beck (1992), as he states that modern society is composed of different institutions which contribute to the production of knowledge and that shape our behavior towards risk. Similarly, insurance is a crucial asset to manage "the everyday world of safety and security" (Ericson & Doyle, 2004). From this research, I deduce that insurers have a significant social responsibility to evaluate and act upon risk. Their decisions have society-wide consequences for the functioning of capital, loss prevention strategies, loss systems and the freedom to take risks. I continue to argue that insurance has similarities to government. First, through contracts, insurers define social

behaviors of their customers. These contracts define what is expected from of the parties' ethical conduct, moral and social responsibility. We saw that insurers stipulate eligibility of coverage based on behavioral conduct and rely heavily on this before deciding who to insure.

In addition, this research has led me to conclude that the insurance industry influences the social well-being of society by adopting moral codes that must be respected. Just as the laws govern our society, policyholders are expected to self-regulate their own behaviors and practices in order to comply with insurers' rules. It can further be argued that the industry adopts these methods to govern from a distance (Ericson & al., 2003). This could be done to reduce the opportunities for some individuals to engage in moral hazards. This is not surprising, as government social controls are also transgressed by individuals.

To counter moral hazards, insurance uses similar policing methods to government. It has a private policing structure, such as investigators, to combat fraud and to prevent loss reductions. Participant 3 mentioned that their clients have access to a 1-800 number when they believe they have been hacked. Amongst many roles, this resource assigns cybercrime professionals to respond to the situation and contain the consequences of the breach or restore one's virtual infrastructure. For this matter, the insurance industry is engaging in a first response approach, like government law enforcement agencies.

However, this does not mean that the state must disengage from governing cybercrimes. For one, the insurance industry is not a law enforcement agency and does not have the ability to legally charge individuals for any type of crime. Rather, as Cauchie and Chantraine (2005) argue, the insurance industry applies a neo-liberal managerial model, which is used to deter individuals from engaging in behaviors that are considered risky. This is in line with Ewald (1991), who mentions that for insurance controls to work, it must be a collective social responsibility of

everyone in the risk pool. This leaves applicants who did not fall within acceptable risk classes without insurance. Furthermore, this leads to the following question: Is it possible that applicants, who are filtered out, will not be able to adopt adequate security measures? I argue that they are more at risk because they might not have the knowledge or the financial strength to enhance their security measures. The governance of cybercrimes needs to also be the responsibility of the state. For example, the government can enact laws and regulations that will impose certain behaviors to adopt on virtual platforms. It's simply not sufficient for the burden to fall in the hands of private institutions; the private and public institutions must work in partnership.

Despite the need for government to actively regulate cybercrimes, there is an absence of concrete law enforcement tools to manage this new reality of crime. I argue that cyber insurance will be able to collect a large sample size of breaches relevant to different industries. I believe that this accumulation of knowledge will allow the insurance industry to profit from partnerships between public and private stakeholders. This is possible because insurance companies have an overview of security requests across various industries (Ericson & Doyle, 2004). Thus, both sectors can consult the insurance industry to better understand what information is most likely sought by attackers. In addition, the insurance industry can suggest what are the most effective measures to reduce the risk of violations. Additionally, the public sector, governments can request insurance companies to provide them with information on breaches. By gaining access to this information, governments can enhance their own infrastructure and consequently, preserve the online safety of their citizens. However, it is important to point out that although the information can used by government, information sharing between the public and private sector needs to be properly administered in order to preserves the insurance industry client's personal information.

CONCLUSION

Using the Grounded Theory developed by Glasser and Strauss (1967), this study initially aimed at studying how insurance companies conceptualize cyber risks to quantify a residual or evolving loss. However, the Grounded Theory brought me to find results that go beyond the conceptualization of cyber risk. As it was suggested, the work of insurance companies goes beyond reducing the financial cost caused by the event of a risk (Elliot. 1960; Mowbray & al., 1979). Ericson and Doyle (2004) make an important distinction. According to these authors, insurance "is a key innovator and participant in communication systems that produce and distribute knowledge of a risk. It takes an active role in the development and implementation of loss prevention infrastructures." (289). Hence, the research revealed that insurance companies are an important tool to understand, manage and govern cyber security.

Due the novelty of cyber insurance, little quantifiable data is available to issue adequate coverage (Yang and Lui, 2014). However, the ongoing work made by the insurance industry is slowly changing this reality. I argued that by constantly working on their policy wording, they are turning the risk into a normality. However, the industry is maintaining risk classifications techniques. In turn, this facilitates the opportunity to commit crime as certain companies do not have the financial backing to strengthen their virtual security and make it harder for attacker to breach their systems.

Understanding of the breach and knowledge accumulation has also been facilitated through an application form used to evaluate a company's cyber security network. This application also facilitates insurers to assume a risk manager role. They do this in two ways. The first, facilitated by Knowledge Diffusion, is to help customers better understand their business data and the security measures to adopt once the application is complete. Following this step, the insurance company

can suggest different strategies and components that can be adopted to make their business operate on a more resilient platform. Among these strategies, insurance companies facilitate the implementation of an IRM plan. This plan will not only help to mitigate security breaches, also reduce the number of people affected.

Finally, the insurance industry, as mentioned by Ericson, Doyle and Barry (2003) are a complement to the governance of new risk. Evidently, the insurance industry adopts similar roles as the states to diminish the chances of clients submitting a claim as well as watching over them from a distance to avoid frauds and moral hazards. These techniques bring their clients to be morally responsible to risk which contributes to the safeguard of their virtual data but the information of their clients as well.

Despite these results, general guidelines when using a Grounded Theory requires an estimated 20 to 30 participants per study. This is required as the goal is to saturate the data (Creswell, 1998). However, this research was only able to benefit from 10 participants. Thus, it can be argued that the data was not properly saturated as there were not enough participants, and they came from only a few positions within the insurance industry. Nonetheless, it is important to note that the field of cyber insurance is relatively new to the market, and not many have specialized in the subject. This considerably reduced our participant pool. Additionally, some refused to take part in the research or ignored the emails altogether; had they not, we would have benefitted from a larger selection. Nevertheless, I suspect that the demand for cyber insurance will increase which will allow future researches to access a larger pool of participants. This would be made possible as the increase in demand will generate a greater number of insurance professionals working with cyber insurance. Moreover, the data collected did not allow me to fully answer my initial question.

I argue that a greater number of participants would allow me to better understand how insurance professionals conceptualize cybercrimes.

Having a larger number of participants would undoubtedly allow for a greater saturation of the data. However, as Ericson and Doyle (2004) mention, "insurers run up against the limits of scientific knowledge and its technical applications" (5). This reality is particularly relevant as technology is developing at a fast pace and making way to new forms of attacks. For this matter, future studies should understand how the new forms of attack generate a level of uncertainty.

When private insurers and governments pool their risks, they usually gather their security needs through discussions of insecurity or past events (Ericson & Doyle, 2004). The rationality of risk assessment is not an accurate calculation. The conceptualization of risk and uncertainty can be accentuated by fear, a rather human emotion. It is important to remember in future research that cybercrime is not only a technological but also a sociological concern. In practice, private insurance companies and governments must go beyond the development of technology-related security measures. Instead, the innovative nature of cybercrime will require them to understand the human dimension of this growing concern.

REFERENCES

Adam, B., Beck, U. & Van Loon, J. (2000). *The Risk Society and Beyond*. London, England: SAGE Publications

Adrian, A. (2010). Beyond Griefing: Virtual Crime. *Computer Law & Security Review, 26*, 640-648.

Allan, J. & Henry, N. (1995). Ulrich Beck's Risk Society at work: Labour and employment in the contract service industries. *Royal Geographical Society*, *22*(2), 180-196.

Avery, L. (2016). *Behind the Numbers: Key Drivers of Cyber Insurance Claims.* Found on https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/aig-claims-intelligence-cyber.pdf

Baker, T. (2002). Risk, Insurance, and the Social Construction of Responsibility. In T.Baker Director & J.Simon (dir.), *Embracing Risk* (p. 33-51). Chicago, Illinois: The University of Chicago Press.

Baker, T. (2003). Containing the Promise of Insurance: Adverse Selection and Risk Classification. In Ericson, R. V. Director & Doyle, A. (dir.), *Risk and Morality* (p. 258-283). Toronto, Ontario: University of Toronto Press.

Baker, T. & Simon, J. (2002). Embracing Risk. In T.Baker Director & J.Simon (dir.), *Embracing Risk* (p. 1-26). Chicago, Illinois: The University of Chicago Press.

Bandyopadhyay, L., Mykytyn, P. P., & Mykytyn, K. (1999). A Fremwork for Integrated Risk Management in Information Technology. *Management Decision*, *37*(5), 437-445.

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT Managers Don't Go for Cyber-Insurance Products. *Communications of the ACM, 52*(11), 68-73.

Baer, W. S., Parkinson, A. (2007). Cyberinsurance in IT Security Management. IEEE Security & Privacy, 50-56.

Bauer, J. M. & van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder Incentives, Externalities and Policy Options. *Telecommunications Policy, 33*, 707-719. doi: 10.1016/j.telpol.2009.09.001.

Beck, U. (1992). *Risk Society: Towards a New Modernity*. London, England: SAGE Publications.

Benoit, W. L. (1997). Image Repair Discourse and Crisis Communication. *Public Relations Review*, *23*(2), 177-186.

Bestak, R., Kencl, L., Li, L. E., Widmer, J. & Yin H. (2012, May). *Networking 2012.* Communication presented at the 11th International IFIP TC 6 Networking Conference, Prague, Czech Republic. Resume found on http://dx.doi.org/10.1007/978-3-642-29066-4_11.

Biener, C., & Eling, M. (2012). Insurability in Microinsurance Markets : An Analysis of Problems and Potential Solutions. The International Association for the Study of Insurance Economics, 37, 77-107.

Biener, C., Eling, M. & Wirfs, J.H. (2015). Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers 40*, 131-158.

Bohme, R., & Schwartz, G. (2010). Modeling Cyber-Insurance: Towards A Unifying Framework. Workshop on the Economics of Information Security (WEIS).

Bolot, J., & Lelarge, M. (2008). Cyber Insurance as an Incentive for Internet Security. *Managing Risk and the Economic of Security.*

Bouzon, A. (2001). Ulrich Beck, La société du Risque. Sur la voie d'une autre modernité, trad. De l'allemand par L.Bernardi. *Question de Communication*, *2*, 1-3.

Bridges, L. (2008). The Changing face of malware. *Network Security*, *2008*(1), 17-20.

Bryant, A. & Charmaz, L. (2007). *The SAGE Handbook of Grounded Theory* (1st ed.). Thousand Oaks, California; SAGE Publications Inc.

Carr, E.C.F. & Worth, A. (2001). The Use of the Telephone Interview for Research. *Journal of Research in Nursing*, *6*(1), 511-524.

Cauchie, J.-F. & Chantraine, G. (2005). Use of Risk in the Government of Crime: New Prudentialism and New Penology. *Champ Pénal/Penal Field*, *2*, 1-13.

Charmaz, K. (2014). Grounded Theory in Global Perspective: Reviews by International Researchers. *Quliatative Inquiry*, *20*(9), 1074-1084.

Choo, K.K.R. (2011). The Cyber Threat Landscape: Challenges and Future Directions. *Computers and Security*, *30*, 719-731.

Colquitt, L. L., Hoyt, R. E., & Lee, R.B. (1999). Integrated Risk Management and the Role of the Risk Manager. *Risk Management and Insurance Review*, *2*(3), 43-61.

Creswell, J. W. (1998). *Qualitative Inquiry and Research Design: Choosing Among Five Traditions* (1st ed.). Thousand Oaks, California: SAGE Publications Inc.

Denzin, N.K. (1992). *Symbolic Interactionism and Cultural Studies*. Oxford, UK & Cambridge, USA: Blackwell.

Drouin, D. (2004). Cyber Risk Insurance. *GIAC Security Essentials Certifications*, *1.4*(1). 1-30.

Eling, M., & Werner, S. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, *17*(5), 474-491.

Elisan, C. C. (2013). *A Beginner's Guide to Malware, Rootkits &Botnets* (1st ed.). New York, New-York: McGraw-Hill.

Elliot, L., Massacci, F. & Williams, J. (2016). Action, Inaction, Trust and Cybersecurity's Common Property Problem. *Security and Privacy Economics*. *14*(1), 82-86.

Elliot, C.M. (1960). *Property and Casualty Insurance*. United-States of America: The McGraw-Hill Book Company, Inc.

Elnagdy, S. A., Qiu, M., & Gai, K. (2016). Cyber Incident Classifications Using Ontology-Based Knowledge Representation for Cybersecurity Insurance in Financial Industry. Communication presented at the 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing. Found on http://ieeexplore.ieee.org/document/7545936/

Ericson, R. V. & Doyle, A. (2003). The Moral Risks of Private Justice: The Case of Insurance Fraud. In Ericson, R. V. Director & Doyle, A. (dir.), *Risk and Morality* (p. 258-283). Toronto, Ontario: University of Toronto Press.

Ericson, R. V. & Doyle, A. (2004). *Uncertain Business: Risk Insurance, and the Limits of Knowledge*. Toronto, Ontario: University of Toronto Press.

Ericson, R. V., Doyle, A. & Barry, D. (2003). *Insurance as Governance*. Toronto, Ontario: University of Toronto Press.

Ericson, R. V. & Haggerty, K.D. (1997). Policing the Risk Society. Toronto, Ontario: University of Toronto Press.

Ericson, R. V. & Haggerty, K.D. (2002). The Policing of Risk. In T.Baker Director & J.Simon (dir.), *Embracing Risk* (p. 239-272). Chicago, Illinois: The University of Chicago Press.

Everett, C. (2016). Ransomware: to pay or not to pay? *Computer Fraud & Security*, *2016*(4), 8-12.

Ewald, F. (1991). Insurance and Risk. In Burchell, G. Director, Gordon, C. (dir.) & Miller, P. (dir.), *The Foucault Effect* (p.197-210). Chicago Illinois: The University of Chicago Press.

Ewald, F. (1996). Philisohphie de la Precaution. *L'année Sociologique*, *46*(2), 383-412.

Flatley, J. (2015). *Crime Statistics, Focus on Property Crime, 2014-2015.* Repéré sur le site Office for National Statistics : http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/focus-on-property-crime--2014-to-2015/index.html.

Gandrud, C. (2014). Competing Risks and Deposit Insurance Governance Convergence. *International Political Science Review*, *35*(2), 195-215.

Garland, D. (2003). The Rise of Risk. In Ericson, R. V. & Doyle, A (dir.), *Risk and Morality* (p. 48-86). Toronto, Ontario: University of Toronto Press.

Gemalto. (2017). *Data Breaches and Customer Loyalty 2017.* Found on https://www6.gemalto.com/2017-data-breaches-customer-loyalty report?utm_source=website&utm_medium=blog&utm_content=customer-loyalty-report&utm_campaign=customer-loyalty-report

Giddens, A. (1999). Risk and Responsibility. *The Modern Law Review*, *62*(1), 1-11.

Glasser, B. G. & Strauss, L. A. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research* (1st ed.). Chicago, Illinois: Aldine Publishing Company.

Gordon, L., Loeb, M. P., Lucyshyn, W. & Zhou, L. (2015). The Impact Information Sharing on Cybersecurity Underinvestment: A Real Option Perspective. *Journal of Accounting and Public Policy*, *34*(5), 509-519.

Gordon, L., Loeb, M., & Sohail, T. (2003). A Framework for Using Insurance for Cyber-Risk Management. *Communications of the ACM, 43*(3), 81-85.

Hacking, I. (2003). Risk and Dirt. In Ericson, R. V. Director & Doyle, A. (dir.), *Risk and Morality* (p. 22-47). Toronto, Ontario: University of Toronto Press.

Han, C., & Dongre, R. 2014. Q&A. What Motivates Cyber-Attackers? *Technology Innovation Management Review*, *4*(10): 40-42.

Heimer, C. (2002). Insuring More, Ensuring Less: The Costs and Benefits of Private Regulation through Insurance. In T.Baker Director & J.Simon (dir.), *Embracing Risk* (p. 117-145). Chicago, Illinois: The University of Chicago Press.

Heimer. C. (2003). Insurers as Moral Actors. In Ericson, R. V. Director & Doyle, A. (dir.), *Risk and Morality* (p. 284-316). Toronto, Ontario: University of Toronto Press.

Hellwege, P. (2016). A Comparative History of Insurance Law in Europe. *American Journal of Legal History*, *56*, 66-75.

Hunton, P. (2009). The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model. *Computer Law & Security Review, 25*, 528-535.

Inshiguro, M., Tanaka, H., Matsuura, K. & Murase, I. (2006). The Effort of Information Security Incidents on Corporate Values in the Japanese Stock Market. *Allen Institute for Artificial Intelligence.*

Insurance Bureau of Canada. (2016). *Getting Started: Managing your risk*. Found on http://assets.ibc.ca/Documents/Brochures/Risk-Management-Getting-started-Process.pdf

Insurance Institute. (2015). *Cyber Risks: Implications for the Insurance Industry in Canada* (Publication n°0-919244-26-2). Toronto, Ontario: The Insurance Institute of Canada.

Keegan, C. (2014). Cyber Security in the Supply Chain: A Perspective from the Insurance Industry. *Technovation, 34*(7), 380-381. doi: http://dx.doi.org/10.1016/j.technovation.2014.02.002.

Kemshall, H. (2006). Crime and Risk. In P.Taylor-Gooby Director and J.Zinn (dir.), *Risk in Social Science* (p.76-93). Oxford, England: Oxford University Press

Kesan, J. P., Majuca, R. P., & Yurcik, W. J. (2004). The Economic Case for Cyberinsurance. *National Center for Supercomputiong Application (NCSA).*

Kim, W., Jeong, O. R., Kim, C. & So, J. (2011). The Dark Side of the Internet: Attacks, Costs and Responses. *Information Systems, 36*(3), 675-705. doi: 10.1016/j.is.2010.11.003.

Kvale, S. & Brinkmann, S. (2009). *Interviews: Learning the Craft of Qualitative Research Interviewing* (2nd ed.). Thousand Oaks, California: SAGE Publications Inc.

Laliberté, D., Rosario, G., Léonard, L., Smith-Moncrieffe, D. & Warner, A. (2015). *Results of Crime Prevention Programs for 12 to 17 Years Olds*. Found on the Public Safety Canada website: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslts-crm-prvntn-12-17/index-eng.aspx.

Landsman, Z., & Sherris, M. (2001). Risk Measures and Insurance Premium Principles. *Insurance Mathematics & Economics*, *29*, 103-115.

Locke, K. (1996). Rewriting the Discovery of Grounded Theory After 25 Years. Journal of Management Inquiry, 5(3), 239-245.

Luzwick, P. (2001). If Most of Your Revenue is From E-Commerce, Then Cyber-Insurance Makes Sense. *Computer Fraud & Security, 2001*(3), 16-17. Doi: 10.1016/S1361-3723(01)03016-0.

Mainelli, M. (2013). Learn from Insurance: Cyber Bore. *The Journal of Risk Finance, 14*(3), 100-102. doi: 10.1108/15265941311288130.

Majuca, R. P., Yurcik, W. & Kesan, J. P. (2006). The Evolution of Cyberinsurance. *University of Illinois at Urbana-Champaign.*

Marsh & Mclennan. (2017). *The Global Risks Report 2017: 12th Edition*. Geneva, Switzerland: World Economic Forum.

Mowbray, A.H., Blanchard, R. H. & Williams, C.A. (1979). *Insurance: Its Theory and Practice in the United States* (6th ed.). Huntington, New York: Robert E. Krieger Publishing Company.

Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection, 3*(4), 103-117. doi: 10.1016/j.ijcip.2010.10.002.

Mukhopadhyay, A., & Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S.K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11-26.

NetDiligence (2016). NetDiligence 2016 Cyber Claims Study. Found on https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf

Neuman, W. L. (2000). *Social Research Methods: Qualitative and Quantitative Approaches* (4th ed.). Needham Heights, Massachusets: Allyn & Bacon.

Office of the Privacy Commissioner of Canada. (2015). *Digital Privacy Act* (Publication n° S.C. 2015, c. 32). Found on http://laws-lois.justice.gc.ca/PDF/2015_32.pdf

Official Journal of the European Union. (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016: Concerning measures for a high common level of security of network and information systems across the Union* (Publication n°I.194/1). Found on http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Ögüt, H., Raghunathan, S. & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis, 31*(3), 497-512. doi: 10.1111/j.1539-6924.2010.01478.x.

O'Malley, P. (2003). Moran Uncertainties: Contract Law and Distinctions between Speculation, Gambling and Insurance. In Ericson, R. V. Director & Doyle, A. (dir.), *Risk and Morality* (p. 231-257). Toronto, Ontario: University of Toronto Press

Opdenakker, R. (2006). Advantages and Disadvantages of Four Interview Techniques in Qualitative Research. *Qualitative Social Research*, *7*(4), 1-13.

Paillé, P. et Mucchielli, A. (2012). L'analyse thématique. Dans Paillé, P. et Mucchielli, A, L'analyse qualitative en sciences humaines et sociales (3e éd, p. 231-314). Paris, France : Armand Colin.

Pal, R. & Hui, P. (2012). Cyber-Insurance for Cyber-Security : A Topological Take on Modulating Insurance Premiums. *Performance Evaluation Review, 40*(3), 86-88.

Pérez, G. M., Mubanga, M., Aznar, Aznar, C. T. & Bagnol, B. (2015). Grounded Theory : A Methodology Choice to Investigating Labia Minora Elongation Among Zambian in South Africa. International Journal of Qualitative Methods, 1-11p. DOI: 10.1177/1609406915618324

Ponemon Institute. (2015). *2015 Cost of Cyber Crime Study: Global Benchmark Study of Global Companies*. Found on the following URL: http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf

Ponemon Institute. (2016). *2016 Cost of Cyber Crime Study & the Risk of Business Innovation: Benchmark Study of 237 Global Companies*. Found on the following URL: https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

Poupart, J. (1997). L'entretien de type qualitatif : considérations épistémologiques, théories et méthodologiques. Dans Poupart, J., Deslauriers, J-P., Grouls, L., Laperrière, A., Mayers, R. et Pires, A. (Eds.), *La recherche qualitative : enjeux épistémologiques et méthodologiques* (p. 198-237). Montréal, Québec: Gaétan Morin

Prefer, I. & Klock, D.R. (1974). *Perspectives on Insurance*. Englewood Cliffs, New Jersey: Prentice-Hall, Inc.

PricewaterhouseCooper. (2017). *Turnaround and Transformation in Cybersecurity: How Canadian Businesses are Responding to Rising Cyber-Risks.* Found on

https://www.pwc.com/ca/en/services/consulting/technology/cyber-resilience/global-state-of-information-security-survey-canadian-insights.html

Raphael, S., & Rice, L. (2002). Car Ownership, Employment and Earning. *Journal of Urban Economics*, *52*, 109-130.

Redja, G. E. (2011). *Principles of Risk Management and Insurance* (11th ed.). United-States of America: Pearson Education Inc.

Rees, L. P., Deane, J. K., Rakes, T. R. & Baker, W. H. (2011). Decision Support for Cybersecurity Risk Planning. *Decision Support Systems, 51*(3), 493-505. doi: 10.1016/j.dss.2011.02.013.

Riegel, R., Miller, J. S. & Williams, C.A. (1976). *Insurance Principles and Practices: Property and Liability* (6th ed.). Englewood Cliffs, New Jersey: Prentice-Hall, Inc.

Robertson, P.L. & Jacobson, D. (2011). Knowledge Transfer and Technological and Technology Diffusion: An Introduction. In P.L.Robertson & D.Jacobson (Eds.), *Knowledge Transfer and Technology Diffusion*. Cheltenham, Gloucestershire: Edward Elgar Publishing Inc.

Shackelford, S.J. (2012). Should your firm Invest in Cyber Risk Insurance? *Business Horizons*, *55*, 349-356.

Siemens, R. & Beck D. (2012). How to Buy Cyber Insurance. *Risk Management.* Article found on http://www.rmmagazine.com/2012/09/28/how-to-buy-cyberinsurance/.

Stevenson, A. (2010). Oxford dictionary of English (3rd ed.). Oxford: Oxford University Press.

Strauss, A. & Corbin, J. (1998). *Basic of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (2nd ed.). Thousand Oaks, London: SAGE Publications Inc.

Suddaby, R. (2006). From the Editors: What Grounded Theory is Not. Academy of Management Journal, 49(4), 633-642.

Vance, W. R. (1908). The Early History of Insurance Law. *Columbia Law Review*, *8*, 1-17.

Van den Hoonaard, D. K. (2012). *Qualitative Research in Action: a Canadian Primer*. Don Mills, ON: Oxford University Press.

Van Loon, J. (2002). *Risk and Technological Culture: Towards a Sociology of Virulence*. London, England: Routledge, Taylor and Francis Group

Vaughan, E. J. & Vaughan, T. M. (2003). *Fundamentals of Risk and Insurance* (9th ed.). United-States of America: John Wiley & Sons, Inc.

Verizon. (2017). *2017 Data Breach Investigations Report 10th Edition.* Found on: https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

Verizon. (2018). *2018 Data Breach Investigations Report 11th Edition*. Found on https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Walsh, I., Holton, J. A., Bailyn, L., Fernandez, N. L. & Glaser, B. (2015). What Grounded Theory Is…A Critically Reflective Conversation Among Scholars. Organisational Research Methods, 18(4), 581-599. DOI: 10.1177/1094428114565028

Willis, A. R. (2010). Business Insurance: First-Party Commercial Property Insurance and the Physical Damage Requirement in a Computer-Dominated World. *Florida State University Law Review*, *37*(4), 1003-1022.

Yang, Z. & Lui J. C. S. (2014). Security Adoption and Influence of Cyber-insurance Markets in Heterogeneous Networks. *Performance Evaluation, 74*, 1-17. doi: 10.1016/j.peva.2013.10.003.

Yu, A. (2014). Let's Get Physical. *Rutgers Computer & Technology Law Journal, 40*, 229-225.

ANNEX I:

TRAVELERS

CyberRisk
Coverage Application

Travelers Insurance Company of Canada

NOTICE

ALL LIABILITY COVERAGE PARTS FOR WHICH APPLICATION IS MADE APPLY, SUBJECT TO THEIR TERMS, ONLY TO "CLAIMS" FIRST MADE OR DEEMED MADE AGAINST "INSUREDS" DURING THE POLICY PERIOD OR ANY EXTENDED REPORTING PERIOD, IF APPLICABLE. THE LIMIT OF LIABILITY AVAILABLE TO PAY LOSSES WILL BE REDUCED BY THE AMOUNTS INCURRED, AS "DEFENCE EXPENSES", AND "DEFENCE EXPENSES" WILL BE APPLIED AGAINST THE RETENTION AMOUNT. THE INSURER HAS NO DUTY TO DEFEND ANY "CLAIM" UNLESS DUTY-TO-DEFEND COVERAGE HAS BEEN SPECIFICALLY PROVIDED HEREIN.

Applicant means all corporations, organizations or other entities, including subsidiaries, proposed for this insurance.

I. GENERAL INFORMATION

1. Name of **Applicant**: _____

Mailing Address: _____

City, Prov., Postal Code: _____

Year Established: _____

Website Home Page Address(es): _____

Applicant Company Type: ☐ Public ☐ Private ☐ Non-Profit ☐ Government

☐ Other (describe) _____

Description of **Applicant's** Operations: _____

_____

Applicant's Standard Industrial Classification (SIC) Code if known (4 digit number):

II. ORGANIZATION/FINANCIAL INFORMATION

1. Subsidiary Information:

Name	Description of Operations	Website Address

Attach a separate sheet if necessary.

2. Are significant changes in the nature or size of the **Applicant's** business anticipated over the next 12 months, or have there been any such changes in the past 12 months? Yes ☐ No ☐
If Yes, please explain: _____

3. Total number of **Applicant's** employees (full and part time including leased, seasonal and temporary): _____

4. Assets/Revenues:

Indicate the following as it relates to the Applicant's fiscal year end (FYE): *(Please indicate negative figures with "( )" or "-" as appropriate)*	**Most Recent FYE (Month/Year) (____/____)**	**Prior FYE (Month/Year) (____/____)**	**Projected FYE (Month/Year) (____/____)**
Total Assets	$	$	$
Total Revenue	$	$	$
Total U.S. Revenue	$	$	$
Indicate the following as it relates to	**Most Recent FYE**	**Prior FYE**	**Projected FYE**

the Applicant's fiscal year end (FYE): *(Please indicate negative figures with "( )" or "-" as appropriate)*	**(Month/Year) (____/____)**	**(Month/Year) (____/____)**	**(Month/Year) (____/____)**
Total Foreign Revenue	$	$	$
Estimated percentage of revenue derived from or dependent upon website or internet	%	%	%

III. REQUESTED INSURANCE TERMS/CURRENT INSURANCE INFORMATION

1. Complete the following table for coverages, limits and retentions requested:

Insuring Agreement	Requested Limit	Requested Retention
A. Network and Information Security Liability (Required)	$	$
B. Communications and Media Liability	$	$
C. Regulatory Defence Expenses	$	$
D. Crisis Event Management Expenses	$	$
E. Security Breach Remediation and Notification Expenses	$	$
F. Computer Program and Electronic Data Restoration Expenses	$	$
G. Computer Fraud	$	$
H. Funds Transfer Fraud	$	$
I. E-Commerce Extortion	$	$
J. Business Interruption and Additional Expenses	$	Waiting Period in Hours

Proposed effective date: _____

2. What is the **Applicant's** preference for defence coverage with respect to Insuring Agreements A., B., and C.? Duty to Defend ☐ Reimbursement ☐

3. If **Applicant** currently has insurance for Errors and Omissions Liability, Network and Security Liability or Media Liability, please provide the following information:

Policy Period	Insurance Company	Limit	Deductible	Retroactive Date	Premium
		$	$		$
		$	$		$

Expiring policy number(s): _____

4. Within the past 3 years, have any of the coverages or similar coverages been declined, cancelled or nonrenewed? Yes ☐ No ☐
If Yes, please provide details: _____

IV. NETWORK SECURITY

SYSTEMS

1. Does the **Applicant** have a designated Chief Security Officer as respects computer systems? Yes ☐ No ☐
If No, please indicate what position is responsible for computer security: _____
2. Does the **Applicant** have a formal program in place to test or audit network security controls? Yes ☐ No ☐
   a. How often are internal audits performed? _____
   b. How often are outside/third party audits performed? _____
3. Does the **Applicant** use firewall technology? Yes ☐ No ☐

4. Does the **Applicant** use anti-virus software? Yes ☐ No ☐

   a. Is anti-virus software installed on all of the **Applicant's** computer systems, including laptops, personal computers, and networks? Yes ☐ No ☐

5. Does the **Applicant** use intrusion detection software to detect unauthorized access to internal networks and computer systems? Yes ☐ No ☐

6. Is it the **Applicant's** policy to upgrade all security software as new releases or improvements become available? Yes ☐ No ☐

7. Does the **Applicant** provide remote access to its network? Yes ☐ No ☐

   a. Is remote access restricted to Virtual Private Networks (VPNs)? Yes ☐ No ☐

8. Is a multi-factor authentication process (multiple security measures used to reliably authenticate/verify the identity of a customer or other authorized user) or a layered security approach required to access secure areas of **Applicant's** website? Yes ☐ No ☐
   Please describe authentication/verification methods used: _____

9. Does the **Applicant** send or accept financial transactions intended for deposit, via the use of remote deposit capture technology (e.g. RDC – Remote Deposit Capture)? Yes ☐ No ☐

10. With respect to computer systems functionality, does the **Applicant** have:

    a. A disaster recovery plan? Yes ☐ No ☐

    b. A business continuity plan? Yes ☐ No ☐

    c. An incident response plan for network intrusions and virus incidents? Yes ☐ ☐

    No How often are such plans tested? _____

11. Does the **Applicant** have secondary computer system or site available if the primary resource becomes inoperative? Yes ☐ No ☐

    a. How long before the secondary resources become operational? _____

    b. What percentage of normal system operations can be handled via the secondary resources? _____

12. Is all valuable/sensitive data backed-up by the **Applicant** on a daily basis? Yes ☐ No ☐
    If No, please describe exceptions: _____

PERSONNEL, POLICIES AND PROCEDURES

1. Does the **Applicant** conduct training regarding security issues and procedures for employees that utilize computer systems? Yes ☐ No ☐

2. Does the **Applicant** publish and distribute written computer and information systems policies and procedures to its employees? Yes ☐ No ☐

3. Does the **Applicant** terminate all associated computer access and user accounts as part of the regular exit process when an employee leaves the company? Yes ☐ No ☐

4. Does the **Applicant** have a formal documented procedure in place regarding the creation and periodic updating of passwords used by employees or customers? Yes ☐ No ☐

V. INFORMATION SECURITY

1. Does the **Applicant** collect, receive, process, transmit, or maintain private, sensitive, or personal information from third parties (i.e. customers, clients, patients) as part of its business activities? Yes ☐ No ☐
   If Yes, please indicate what type:

   ☐ Credit/Debit Card Data ☐ Medical Information ☐ Bank Accounts and Records Social Insurance/Security Numbers ☐ Employee/HR Information ☐ Customer Information

   ☐ Intellectual Property of others ☐ Other _____

a. Does the **Applicant** have written procedures in place to comply with laws governing the handling or disclosure of such information? Yes ☐ No ☐

b. Does the **Applicant** share private, sensitive, or personal information gathered from customers (by the **Applicant** or others) with third parties? Yes ☐ No ☐

2. At any one time, approximately how many individual records containing one or more items of the information listed above does the **Applicant** have stored?

☐	<1,000	☐	1,000,001 to 3,000,000
☐	1,000 to 10,000	☐	3,000,001 to 5,000,000
☐	10,001 to 100,000	☐	5,000,001 to 7,000,000
☐	100,001 to 500,000	☐	7,000,001 to 10,000,000
☐	500,001 to 1,000,000	☐	>10,000,000

3. Is user-specific, private, sensitive or confidential information stored on **Applicant's** server(s) encrypted? Yes ☐ No ☐

4. Is user-specific, private, sensitive or confidential information stored on portable communications equipment (e.g., laptops, BlackBerry devices, PDAs, USB Flash Drives, or other portable devices)? Yes ☐ No ☐

a. If yes, does **Applicant** have a company policy or procedure for the secure care, handling and storage of private, sensitive or confidential information on portable communications devices? Yes ☐ No ☐

b. If yes, what percentage of user-specific, private, sensitive or confidential information stored on portable communications devices is encrypted? _____ %

5. Does the **Applicant** require service providers who may have access to the **Applicant's** confidential information or personally identifiable information to demonstrate adequate security policies and procedures? Yes ☐ No ☐

a. Are service providers required by contract to indemnify the **Applicant** for harm arising from a breach of the provider's security? Yes ☐ No ☐

VI. WEBSITE AND CONTENT INFORMATION

Website (Check all that apply)	Current	Within Next 12 Months
Information website only provides general information about the **Applicant's** products/services	☐	☐
Accessible website has log-in capabilities allowing access to secure or restricted content (e.g., accounts, subscriptions, or profiles) and/or allows user to upload or download secure data	☐	☐
Transactional website allows orders or purchases using credit card, debit card, or bill-pay payment	☐	☐
View account balances or statements	☐	☐
Transfer funds between accounts	☐	☐
Bill payment	☐	☐

1. Does **Applicant's** website contain, disseminate, employ or allow the following? *Please check all that apply:*

☐ Music/Sound clips	☐ Chat Rooms/Message Boards/Blogs	☐ Executable programs or shareware
☐ Movies/Movie clips	☐ Advertising of others	☐ Interactive gaming/games of chance
☐ Sweepstakes or coupons	☐ Sexually explicit material	☐ Content specifically targeted at minors

2. Does the **Applicant** have a written intellectual property clearance procedure for content disseminated via the **Applicant's** website? Yes ☐ ☐ No Do the procedures include the following:

a. Review of content by qualified lawyer? Yes ☐ No ☐

b. Screening the content for the following:

i. Disparagement issues? Yes ☐ No ☐

ii. Copywriting infringement? Yes ☐ No ☐

iii Trademark infringement? Yes ☐ No ☐

iv. Invasion of privacy? Yes ☐ No ☐

a. Obtaining agreements with outside developers or consultants that include provisions granting the **Applicant** ownership of the intellectual property rights and business methods incorporated into any work for hire performed by or on behalf of the **Applicant**? Yes ☐ No ☐

b. Requiring employees and independent contractors to sign a statement that they will not use previous employers' or clients' trade secrets or other intellectual property? Yes ☐ No ☐

c. Obtaining written permission of any website the **Applicant** links to or frames? Yes ☐ No ☐

2. If the **Applicant** does not have a process to review all content prior to posting, please describe procedures to avoid the posting of improper or infringing content: _____

_____

_____

3. Does **Applicant** have a formal procedure for editing or removing controversial, offensive or infringing material from material distributed, broadcast or published by or on behalf of the **Applicant**? Yes ☐ No ☐

4. Does **Applicant** collect data about children who use your website? Yes ☐ No ☐
If Yes, please describe the method used to obtain parental permission: _____

6. Does the **Applicant** have a procedure for responding to allegations that content created, displayed or published by the **Applicant** is libelous, infringing, or in violation of a third party's privacy rights? Yes ☐ No ☐

7. Has the **Applicant** screened all trademarks used by the **Applicant** for infringement with existing trademarks prior to first use? Yes ☐ No ☐

a. Has the **Applicant** acquired any trademarks from others in the past 3 years? Yes ☐ No ☐
If Yes, were acquired trademarks screened for infringement? Yes ☐ No ☐

VII. LOSS INFORMATION

In the past 3 years:

1. Has the **Applicant** ever received any claims or complaints, or been subject to any government action, investigation or subpoena with respect to allegations of failing to prevent unauthorized access to confidential information, failing to notify appropriate individuals of any such unauthorized access or failing to allow authorized users access to the **Applicant's** computer systems? Yes ☐ No ☐

2. Has the **Applicant** ever received any claims or complaints, or been subject to any government action, investigation or subpoena with respect to allegations that any content disseminated on or via the **Applicant's** websites or company email, infringed on the intellectual property rights of another party or caused harm to the reputation of another party? Yes ☐ No ☐

If question 1 or 2 is answered Yes, provide details below of each claim, complaint, allegation or incident, including costs, losses or damages incurred or paid, any corrective procedures to avoid such allegations in the future and any amounts paid as a loss under any insurance policy.

Date of Such Claim/Complaint	Nature of Claim/Complaint	Amount Paid for Defence	Amount Sought or Paid for Damages	Covered by Insurance?	Corrective Procedures Implemented	Current Status
		$	$	Yes ☐ No ☐		
		$	$	Yes ☐ No ☐		
		$	$	Yes ☐ No ☐		

To enter more information, please attach a separate page to the Application.

3. Has the **Applicant** ever experienced an extortion attempt or demand with respect to its computer systems, or suffered a loss of money, securities or other property due to fraud

committed by means of unauthorized or fraudulently entered computer instructions or code by someone other than an employee? Yes ☐ No ☐
If Yes, please provide details: _____

3. Has the **Applicant** suffered any known intrusions (i.e., unauthorized access or security breach) or denial of service attacks which impaired the functionality of its computer systems? Yes ☐ No ☐
If Yes, please provide details: _____

4. Is the **Applicant** or any person proposed for this insurance aware of any fact, circumstance, situation, event or act that reasonably could give rise to a claim against them under the insurance policy for which the **Applicant** is applying? Yes ☐ No ☐
If Yes, please provide details: _____

*With respect to the information required to be disclosed in response to the questions above, the proposed insurance will not afford coverage for any claim arising from any fact, circumstance, situation, event or act about which any executive officer of the **Applicant** had knowledge prior to the issuance of the proposed policy, nor for any person or entity who knew of such fact, circumstance, situation, event or act prior to the issuance of the proposed policy.*

VIII. REQUIRED ATTACHMENTS

- Most current audited or annual financial statements if annual revenues exceed $10,000,000 or requested Limit of Liability for Network and Information Security Liability coverage exceeds $3,000,000.

*If additional space is needed to address certain questions, attach additional sheets on **Applicant's** letterhead as necessary.*

XI. SIGNATURE SECTION

THE UNDERSIGNED AUTHORIZED REPRESENTATIVE (PRESIDENT, CEO, CHIEF INFORMATION/SECURITY OFFICER OR OTHER OFFICER ACCEPTABLE TO TRAVELERS) OF THE APPLICANT DECLARES THAT TO THE BEST OF HIS/HER KNOWLEDGE AND BELIEF, AFTER REASONABLE INQUIRY, THE STATEMENTS SET FORTH IN THE ATTACHED TRAVELERS NEW BUSINESS OR RENEWAL APPLICATION FOR INSURANCE ARE TRUE AND COMPLETE AND MAY BE RELIED UPON BY TRAVELERS. IF THE INFORMATION IN ANY APPLICATION CHANGES PRIOR TO THE INCEPTION DATE OF THE POLICY, THE APPLICANT WILL NOTIFY THE INSURER OF SUCH CHANGES, AND THE INSURER MAY MODIFY OR WITHDRAW ANY OUTSTANDING QUOTATION. THE INSURER IS AUTHORIZED TO MAKE INQUIRY IN CONNECTION WITH THIS APPLICATION.

THE SIGNING OF THIS APPLICATION DOES NOT BIND THE INSURER TO OFFER, NOR THE APPLICANT TO PURCHASE, THE INSURANCE. IT IS AGREED THAT THIS APPLICATION, INCLUDING ANY MATERIAL SUBMITTED THEREWITH, SHALL BE THE BASIS OF THE INSURANCE AND SHALL BE CONSIDERED PHYSICALLY ATTACHED TO AND PART OF THE POLICY, IF ISSUED. THE INSURER WILL HAVE RELIED UPON THIS APPLICATION, INCLUDING ANY MATERIAL SUBMITTED THEREWITH, IN ISSUING THE POLICY.

REPRODUCED SIGNATURES WILL BE TREATED AS ORIGINAL.

Signature * of **Applicant's** Authorized Representative (President, CEO or Chief Information/Security Officer)	Name (Printed)
Title	Date

Reset Form Print Form

ANNEX II:

NOTICE

The policy for which you are applying is written on a claims made and reported basis. Only claims first made against the insured and reported to the insurer during the policy period or extended reporting period, if applicable, are covered subject to the policy provisions. The limits of liability stated in the policy are reduced, and may be exhausted, by claims expenses. Claims expenses are also applied against your retention, if any. If a policy is issued, the application is attached to and made a part of the policy so it is necessary that all questions be answered in detail.

INSTRUCTIONS

Please respond to answers clearly. Underwriters will rely on all statements made in this application. This form must be dated and signed by the CEO, CFO, President, Risk Manager or General Counsel. Completion of this submission may require input from your organization's risk management, information technology, finance, and legal departments:

Please note that you may be asked to provide the following information as part of the underwriting process:

- Security Supplemental Application based on certain revenue or record counts (over $500mm in annual revenues or over 2mm Privacy Information records)
- Most recent annual report, 10K or audited financials
- List of all material litigation threatened or pending (detailing plaintiff's name, cause(s) of action/allegations, and potential damages) which could potentially affect the coverage for which applicant is applying
- Descriptions of any acts, errors or omissions which might give rise to a claim(s) under the proposed policy
- Loss runs for the last five years
- Copy of your in-house corporate privacy policy(ies) currently in use by your organization

NEED HELP

If you have any questions about the items asked in this form, please contact your broker or agent. An ACE underwriter can also be made available to discuss the application.

Part 1 – Company Information	
Company Name Click here to enter text.	Address (City, State, Zip) Click here to enter text.
Applicant Name Click here to enter text.	Title Click here to enter text.
Email Address Click here to enter text.	Phone Click here to enter text.
Company Type Click here to enter text.	Primary Industry Please select
Years Established Click here to enter text.	Number of Employees Click here to enter text.
Last 12 months gross revenues (% online if applicable) Click here to enter text.	Projected 12 months gross revenue (% online if applicable) Click here to enter text.
Primary Company Website(s) Click here to enter text.	Operates outside of the United States Please select

Part 2 – Information Privacy and Governance. Which of the following types of Privacy Information (Personal Information or Third Party Corporate Information) does your company store, process, transmit or is otherwise responsible for securing? Please indicate total number of records (if known) inclusive of both internal staff or 3rd parties:		
a. Government issued identification numbers (e.g., social security numbers) Comments	☐Yes ☐No	# of records
b. Credit card numbers, debit card numbers or other financial account numbers Comments	☐Yes ☐No	# of records
c. Healthcare or medical records Comments	☐Yes ☐No	# of records
d. Intellectual property (e.g., third party intellectual property trade secrets, M&A information) Comments	☐Yes ☐No	# of records
e. Usernames and passwords Comments	☐Yes ☐No	# of records
f. Does the company maintain a data classification and data governance policy? ☐Yes ☐No Comments		
g. Does the company maintain documentation that clearly identifies the storage and transmission of all Privacy Information? ☐Yes ☐No Comments		
h. When was the company's privacy policy last reviewed? as of (date)		
i. (Optional) Additional comments regarding the Information Privacy and Governance: Click here to enter text.		

Which are the following statements are valid as it relates to Privacy Information Governance. Use the comments for clarification as needed.	
j. Does your company encrypt Privacy Information when:	
1. Transmitted over public networks (e.g., the Internet) Comments	☐Yes ☐No
2. Stored on mobile assets (e.g., laptops, phones, tablets, flash drives) Comments	☐Yes ☐No
3. Stored on enterprise assets (e.g., databases, file shares, backups) Comments	☐Yes ☐No
4. Stored with 3rd party services (e.g., cloud) Comments	☐Yes ☐No
k. Does your company store Privacy Information on a secure network zone that is segmented from internal network Comments	☐Yes ☐No
l. (Optional) What other technologies are used to secure Privacy Information (e.g., tokenization)? Click here to enter text.	
m. (Optional) Additional comments regarding the Privacy Information Governance: Click here to enter text.	

Part 3 - Security Organization		
a. Does your company have an individual designated for overseeing information *security*? ☐Yes ☐No Please enter names and titles		
b. Does your company have an individual designated for overseeing information *privacy*? ☐Yes ☐No		
c. Is your company compliant with any of the following regulatory or compliance frameworks (please check all that apply and indicate most recent date of compliance):		
☐ ISO17999 as of (date) ☐ SOX as of (date) ☐ PCI-DSS as of (date)	☐ HITECH as of (date) ☐ HIPAA as of (date) ☐ GLBA as of (date)	☐ SSAE-16 as of (date) ☐ FISMA as of (date) ☐ Other Click here to enter text.
d. Does your company leverage any industry security frameworks for confidentiality, integrity and availability (e.g., NIST, COBIT)? Click here to enter text.		
e. Is your company an active member in outside security or privacy groups (e.g., ISAC, IAPP, ISACA)? Click here to enter text.		
f. (Optional) What percentage of the overall IT budget is allocated for security? Click here to enter text.		
g. (Optional) Additional comments regarding the Information Security Organization: Click here to enter text.		

Part 4 - Information Security. Use the comments field for clarification as needed.	
a. Does the company have a formal risk assessment process that identifies critical assets, threats and vulnerabilities? Comments	☐Yes ☐No
b. Does the company have a disaster recovery and business continuity plan? Comments	☐Yes ☐No
c. Does the company have an Incident Response Plan for determining the severity of a potential data security breaches and providing prompt notification to all individuals who may be adversely affected by such exposures? Comments	☐Yes ☐No
d. Does the company have an intrusion detection solution that detects and alerts an individual or group responsible for reviewing malicious activity on the company network? Comments	☐Yes ☐No
e. Does the company configure firewalls to restrict inbound and outbound network traffic to prevent unauthorized access to internal networks? Comments	☐Yes ☐No
f. Does the company perform reviews at least annually of the company's third-party service providers to ensure they adhere to company requirements for data protection? Comments	☐Yes ☐No
g. Does the company use multi-factor authentication for remote network access originating from outside the company network by employees and third parties (e.g., VPN, remote desktop)? Comments	☐Yes ☐No
h. Does the company conduct security vulnerability assessments to identify and remediate critical security vulnerabilities on the internal network and company public websites on the Internet? Comments	☐Yes ☐No
i. Does the company install and update an anti-malware solution on all systems commonly affected by malicious software (particularly personal computers and servers)? Comments	☐Yes ☐No
j. Does the company use any software or hardware that has been officially retired (i.e., considered "end-of-life") by the manufacturer (e.g., Windows XP)? If Yes, please list software	☐Yes ☐No
k. Does the company update (e.g., patch, upgrade) commercial software for known security vulnerabilities per the manufacturer advice? Comments	☐Yes ☐No
l. Does the company update open source software (e.g., Java, Linux, PHP, Python, OpenSSL) that is not commercially supported for known security vulnerabilities? Comments	☐Yes ☐No
m. Does the company have processes established that ensure the proper addition, deletion and modification of user accounts and associated access rights? Comments	☐Yes ☐No
n. Does the company enforce passwords that are at least seven characters and contain both numeric and alphabetic characters? Comments	☐Yes ☐No
o. Does the company require annual security awareness training for all personnel so they are aware of their responsibilities for protecting company information and systems? Comments	☐Yes ☐No
p. Does the company screen potential personnel prior to hire (e.g., background checks include previous employment history, drug, criminal record, credit history and reference checks)? Comments	☐Yes ☐No
q. Does the company have a solution to protect mobile devices (e.g., Laptops, iPhones, iPads, Android, Tablets) to prevent unauthorized access in the event the device is lost or stolen? Comments	☐Yes ☐No
r. Does the company have entry controls that limit and monitor physical access to company facilities (e.g., offices, data centers, etc.)? Comments	☐Yes ☐No

Part 5 – Third Party Technology Services (e.g., cloud, web hosting, co-location, managed services)	
a. Is there an individual responsible for the security of the company information that resides at third party technology service providers? Click here to enter text.	☐Yes ☐No
b. Do your third party technology service providers meet required regulatory requirements that are required by your company (e.g., PCI-DSS, HIPAA, SOX, etc.)?	☐Yes ☐No
c. Does your company perform assessments or audits to ensure third party technology providers meet company security requirements? If Yes, when was the last audit completed? Select date	☐Yes ☐No
d. Does your company have a formal process for reviewing and approving contracts with third party technology service providers?	☐Yes ☐No
e. (Optional) Additional comments regarding the Third Party Technology Services: Click here to enter text.	☐Yes ☐No

Part 6 - Current Network & Technology Providers (if applicable and required at time of binding)	
Internet Communication Services Click here to enter text.	Credit Card Processor(s) Click here to enter text.
Website Hosting Click here to enter text.	Other Providers (e.g., Human Resource, Point of Sale) Click here to enter text.
Collocation Services Click here to enter text.	Anti-virus Software Click here to enter text.
Managed Security Services Click here to enter text.	Firewall Technology Click here to enter text.
Broadband ASP Services Click here to enter text.	Intrusion Detection Software Click here to enter text.
Outsourcing Services Click here to enter text.	Cloud Services (e.g., Amazon, Salesforce, Office365) Click here to enter text.

Please complete the following information for cloud services you process or store Privacy Information. Use the optional comments if more space is required:

Cloud Provider	Type	Service	# of Records	Encrypted Storage
Click here to enter text.	Select	Select	Click here to enter text.	Select
Click here to enter text.	Select	Select	Click here to enter text.	Select
Click here to enter text.	Select	Select	Click here to enter text.	Select

(Optional) Additional comments regarding cloud services: Click here to enter text.

Part 7 – Internet Media Information (only required if Internet Media Coverage is being requested)	
a. Please list the domain names for which coverage is requested: Click here to enter text.	
b. Has legal counsel screened the use of all trademarks and service marks, including your use of domain names and metatags, to ensure they do not infringe on the intellectual property of others? Comments	☐Yes ☐No
c. Do you obtain written permissions or releases from third party content providers and contributors, including freelancers, independent contractors, and other talent? Comments	☐Yes ☐No
d. Do you require indemnification or hold harmless agreements from third parties (including outside advertising or marketing agencies) when you contract with them to create or manage content on your behalf? Comments	☐Yes ☐No
e. If you sell advertising space on any of your websites, are providers of advertisements required to execute indemnification and hold harmless agreements in your favor? Comments	☐Yes ☐No ☐n/a
f. Have your privacy policy, terms of use, terms of service, and other customer policies been reviewed by counsel? Comments	☐Yes ☐No
g. Do you involve legal counsel in reviewing content prior to publication or in evaluating whether it should be removed when notified that content is defamatory, infringing, in violation of a third party's privacy rights, or otherwise improper? Comments	☐Yes ☐No
h. Does your website include content directed at children under the age of 18? Comments	☐Yes ☐No
i. Do you collect data about children who use your website? Do you obtain parental consent regarding your collection of data about children who use your website? Comments	☐Yes ☐No
j. Please describe your company's process to review content prior to publication to avoid the posting, publishing or dissemination of content that is defamatory, infringing, in violation of a third party's privacy rights or otherwise: Click here to enter text.	
k. Please describe your review and takedown procedure when notified that content is defamatory, infringing, in violation of a third party's privacy rights or otherwise improper: Click here to enter text.	
l. (Optional) Additional comments regarding the Internet Media Information: Click here to enter text.	

Part 8 - Current Loss Information. In the past *5 years* has the company ever experienced any of the following events or incidents? Please check all that apply. Please use the comments below to describe any current losses.	
a. Company was declined for Privacy, Cyber, Network, or similar insurance, or had an existing policy cancelled *(Missouri applicants do not answer this question)* Comments	☐Yes ☐No
b. Company, its directors, officers, employees or any other person or entity proposed for insurance has knowledge of any act, error or omission which might give rise to a claim(s) under the proposed policy Comments	☐Yes ☐No
c. Company has been the subject of an investigation or action by any regulatory or administrative agency for violations arising out of your advertising or sales activities Comments	☐Yes ☐No
d. Company sustained a loss of revenue due to a systems intrusion, denial-of-service, tampering, malicious code attack or other type of cyber attack Comments	☐Yes ☐No
e. Company had portable media (e.g., laptop, backup tapes) that was lost or stolen and was not encrypted Comments	☐Yes ☐No
f. Company had to notify customers or offer credit monitoring that their personal information was or may have been compromised as a result of the your activities Comments	☐Yes ☐No
g. Company received a complaint concerning the content of the company website or other online services related to intellectual property infringement, content offenses, or advertising offenses Comments	☐Yes ☐No
h. Company sustained an unscheduled network outage that lasted over 24 hours Comments	☐Yes ☐No
i. (Optional) Additional comments regarding Current Loss Information: Click here to enter text.	

Part 9: Current Coverage. Which of the following policies does the company currently have in force:	
☐ General Liability Policy	☐ Cyber / Privacy Liability Policy
☐ D&O Policy	☐ Other Related Policy (not listed)
☐ Professional Liability	☐ Crime
(Optional) Additional comments regarding Current Coverage: Click here to enter text.	

FRAUD WARNING STATEMENTS

NOTICE TO ALABAMA APPLICANTS: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to restitution fines or confinement in prison, or any combination thereof.

NOTICE TO ARKANSAS, LOUISIANA, RHODE ISLAND AND WEST VIRGINIA APPLICANTS: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

NOTICE TO COLORADO APPLICANTS: It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance, and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Colorado Division of Insurance within the Department of Regulatory Agencies.

NOTICE TO DISTRICT OF COLUMBIA APPLICANTS: WARNING: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits, if false information materially related to a claim was provided by the applicant.

NOTICE TO FLORIDA APPLICANTS: Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete or misleading information is guilty of a felony of the third degree.

NOTICE TO KANSAS APPLICANTS: Any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act.

NOTICE TO KENTUCKY APPLICANTS: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.

NOTICE TO MAINE APPLICANTS: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or a denial of insurance benefits.

NOTICE TO MARYLAND APPLICANTS: Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

NOTICE TO MINNESOTA APPLICANTS: A person who submits an application or files a claim with intent to defraud or helps commit a fraud against an insurer is guilty of a crime.

NOTICE TO NEW JERSEY APPLICANTS: Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

NOTICE TO NEW MEXICO APPLICANTS: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to civil fines and criminal penalties.

NOTICE TO NEW YORK APPLICANTS: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime, and shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

NOTICE TO OHIO APPLICANTS: Any person who, with intent to defraud or knowing that he/she is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

NOTICE TO OKLAHOMA APPLICANTS: WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for the proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

NOTICE TO OREGON APPLICANTS: Any person who knowingly and with intent to defraud any insurance company or another person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading information concerning any fact material thereto, may be committing a fraudulent insurance act, which may be a crime and may subject the person to criminal and civil penalties.

NOTICE TO PENNSYLVANIA APPLICANTS: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

NOTICE TO VERMONT APPLICANTS: Any person who knowingly presents a false statement in an application for insurance may be guilty of a criminal offense and subject to penalties under state law.

NOTICE TO TENNESSEE, VIRGINIA AND WASHINGTON APPLICANTS: It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

NOTICE TO ALL OTHER APPLICANTS: Any person who knowingly and with intent to defraud any insurance company or another person, files an application for insurance or statement of claim containing any materially false information, or conceals information for the purpose of misleading, commits a fraudulent insurance act, which is a crime and may subject such person to criminal and civil penalties

DECLARATION AND CERTIFICATION

SIGNATURE – FOR ALL APPLICANTS (REQUIRED)

Signed: _____(must be Officer of Applicant)
Print Name & Title: _____
Date (MM/DD/YY): _____
Email/Phone: _____

SIGNATURE - FOR ARKANSAS, MISSOURI, AND WYOMING APPLICANTS ONLY

PLEASE ACKNOWLEDGE AND SIGN THE FOLLOWING DISCLOSURE TO YOUR APPLICATION FOR INSURANCE:

I understand and acknowledge that the policy for which i am applying contains a defense within limits provision which means that claims expenses will reduce my limits of liability and may exhaust them completely. Should that occur, I shall be liable for any further claims expenses and damages.

Applicant's Signature (Arkansas, Missouri, & Wyoming Applicants, In Addition To Application Signature Above):

Signed: _____(must be Officer of Applicant)
Print Name & Title: _____
Date (MM/DD/YY): _____
Email/Phone: _____

FOR FLORIDA APPLICANTS ONLY:

Agent Name: _____
Agent License ID Number: _____

FOR IOWA APPLICANTS ONLY:

Broker: _____
Address: _____