Cyber Insurance and Risk Management: A Normative Analysis

Kai-Lung Hui, Wendy Wan-Yee Hui, Wei Thoo Yue

Nov 14, 2019

Abstract

Cyber insurance is becoming an essential tool for managing cybersecurity risks. In this study, we analyze how cyber insurance affects firms' risk prevention and risk mitigation decisions. We find that the presence of cyber insurance exacerbates *ex-ante* moral hazard by decreasing expected risk prevention but enhances *ex-post* efforts by increasing expected risk mitigation. The overall impact of cyber insurance on the risk accepted by a firm depends on the scope and compensation of the insurance coverage. Specifically, a firm will accept a lower level of risk if the cyber insurance covers fewer types of events but provides more compensation when a breach occurs. We discuss the implications of our findings.

Keywords: Risk management, risk prevention, post-breach risk mitigation, cyber insurance, insurance coverage

1. Introduction

According to International Data Corporation, the amount that firms spend on security continues to increase and is expected to rise from $73.7 billion in 2016 to $101.6 billion in 2020.[1] Firms use a multitude of security counter measures to address cybersecurity risks. As cyber-attacks continue to evolve, cyber insurance has emerged as one alternative risk management measure. The global cyber insurance market is expected to grow to $10 billion in annual premiums by 2020 (Merrey et al. 2017). Currently, an estimated 2,000 to 3,000 types of cyber insurance policies exist in the United States, covering a wide variety of

[1] For details, see http://www.idc.com/getdoc.jsp?containerId=prUS41851116

cybersecurity risks such as data compromise response, cyber extortion, and public relations services (Romanosky et al. 2019).

Firms use cyber insurance to contain their losses from cybersecurity attacks or security breach incidents. For example, Capital One suffered a massive data breach affecting 100 million individuals in the summer of 2019. The company had $400 million cyber insurance coverage with a $10 million deductible. The company eventually suffered a significantly reduced data breach cost in the range of $100 to $150 million after the cyber insurance compensation (Surane and Nguyen 2019).

To appreciate the merit of cyber insurance, we must analyze its compatibility and interaction with other cybersecurity investment decisions. As demonstrated by countless real-world incidents, a firm's decisions on cybersecurity are not restricted to *ex-ante* breach incident prevention; *ex-post* breach incident mitigation is an important step in minimizing a breach's impacts.[2] In the Capital One incident, the company's vulnerability disclosure program detected the breach not long after it occurred (12 days, as compared to the average of 297 days in other security breach incidents), allowing the company to react to the incident swiftly (Otto 2019). The interactions between cyber insurance and a firm's *ex-ante* risk prevention effort and *ex-post* risk mitigation effort are an important area of study, and are the focus of this research.

Previous studies have reached mixed conclusions about the influence of cyber insurance on a firm's risk prevention effort (Gordon, Loeb and Sohail 2003, Bolot and Lelarge 2008). Even less research has been conducted on how cyber insurance affects a firm's risk mitigation efforts. Like other types of insurance, cyber insurance could introduce moral hazard. The insured firm might increase risk-taking actions at the expense of the insurer because the insurer cannot observe the firm's actions.

The economics literature has considered the impact of insurance on the insured's behavior. In particular, Ehrlich and Becker (1972) distinguish the insured's action to reduce the size of a loss (self-

[2] Incidentally, there has been a call to shift from the traditional risk prevention model, the so-called "Mottle and Bailey" model, to a risk mitigation-based "cyber immune system" model (Burrows 2017).

insurance) from the action to reduce the probability of loss (self-protection).[3] For example, a sprinkler system serves as a self-insurance measure because it reduces the loss from fire. In contrast, a burglar alarm is a self-protection measure because it prevents illegal entries. Ehrlich and Becker find that an insurance underwritten by external parties ("market insurance") tends to substitute self-insurance, but it may complement self-protection if the probability of loss is large. Self-insurance is a form of risk mitigation because it reduces the severity of an incident. However, in this stream of economic research, the cost of self-insurance occurs *before* the incident. In the cybersecurity context, risk mitigation measures are often invoked *after* the incident. This is our key point of departure from the literature.

Our analysis shows that this fundamental difference, that the insured firm expends effort on risk mitigation *after* a security incident, results in a distinctive interaction with cyber insurance. Specifically, we find that cyber insurance encourages risk mitigation but discourages risk prevention; i.e., it aggravates *ex-ante* moral hazard but enhances *ex-post* effort investment. This result is akin to what has been observed in the health insurance literature, where full insurance discourages preventive care because the cost of illness treatment is covered—the classical moral hazard problem. Co-insurance is the force ("stick") that can alleviate this problem, and incentive plans (rebates) are the "carrot" that induces a more healthy lifestyle to prevent illness (Heffley and Miceli 1998). In cyber insurance, perhaps due to the complexity of cyber-attacks, incentive plans are rarely adopted. Usually, the insurer underwrites outcomes for different types of security incidents. For example, some firms are more concerned about customer data breaches, whereas others are worried about IT service availability.

In our analysis, we scrutinize two common features of cyber insurance: the number of items covered and co-insurance rate. We call the number of items covered the "scope" of the policy: it details the types of incidents covered, e.g., losses due to data theft, cyber extortion, and damages to digital assets (Marotta et al. 2017). We do not differentiate first-party liability and third-party liability, which may result from litigation, fines, and settlement costs payable to third parties that suffer due to the security incident, because

[3] Here, action refers to an investment or effort made by the insured party.

any third-party damage will be borne by a firm without insurance coverage. Therefore, technically, any indemnity against third-party losses is equivalent to insuring against first-party damages.

Co-insurance rate is related to the concept of "depth." An insurance policy with a higher depth provides more compensation when an adverse event, such as a cybersecurity breach, occurs. The extent of compensation is directly determined by the co-insurance rate. The higher the co-insurance rate, the lower the depth and hence the lower the compensation the insured firm receives.

We find, somewhat surprisingly, that cyber insurance can most effectively decrease the overall risk to an insured firm if the insurance coverage is sufficiently deep or the scope is sufficiently narrow. A higher depth in insurance coverage motivates the firm to spend more on risk mitigation because of increasing returns on spending. Contrary to the common intuition that co-insurance curbs the abuse of insurance, a low co-insurance rate actually motivates responsible resolutions of the security incidents. Similarly, a narrower scope motivates the firm to invest in *ex-ante* risk prevention, which increases the net marginal benefit of *ex-post* risk mitigation efforts. Intuitively, to reduce the overall residual risk, we must ensure that the *ex-ante* moral hazard (i.e., the firm's tendency to reduce risk prevention) is not too large, which can be facilitated by trimming the scope of the cyber insurance coverage.

Our analysis provides novel and normative insights into how cyber insurance affects the welfare of a firm and its consumers by distorting the firm's efforts in *ex-ante* risk prevention and *ex-post* risk mitigation. Although procuring cyber insurance could reduce risk prevention due to moral hazard, trimming its scope and extending its depth can lead to more efforts in risk mitigation, which serves as a balancing force to decrease the overall risk of the insured firm.

The rest of this paper is organized as follows. Section 2 reviews the literature. Section 3.1 describes and analyzes a baseline two-stage model in which the risk prevention decision is made before the security incident, and the risk mitigation decision is made after the incident. Section 3.2 adds cyber insurance to the baseline model. Section 4 discusses the managerial implications of our findings. Section 5 identifies a few future research directions and concludes the paper.

2. Literature Review

Our work is related to two streams of information security research: cyber insurance and moral hazard, and risk management strategies for risk prevention and risk transfer.

2.1 Cyber Insurance and Moral Hazard

Studies of cyber insurance examine its slow uptake from different perspectives, such as system interdependence (Kunreuther and Heal 2003), correlated risks (Bohme 2005, Bohme and Kataria 2006), information asymmetry (Bandyopadhyay et al. 2008), and information sharing and cyber insurance selection (Bodin et al. 2018). The closest related work is by Ogut et al. (2011), who find that cyber insurance coverage and risk prevention spending can either be substitutes or complements depending on whether the insurer can design a contract contingent on the firm's risk prevention level. Bolot and Lelarge (2008) show that cyber insurance can complement risk prevention strategies. Gordon, Loeb and Sohail (2003) find that cyber insurance reduces a firm's own efforts in risk prevention. Pal et al. (2014) show that the merit of cyber insurance depends on its market structure.

In the insurance literature, most studies after Arrow (1963) and Pauly (1968) focus on *ex-ante* moral hazard (Rowell and Connelly 2012). For example, in third-party car insurance, the driver at fault often needs to pay for the repair of *all* of the damages to the other party's car. *Ex-post* decisions of the insured driver are moot. Cyber insurance is different from general insurance because the insured firm often needs to make *ex-post* efforts to contain the losses. For example, after a data breach, a bank can re-issue customers' credit cards to minimize fraudulent transactions due to the lost card numbers.

In other contexts, the *ex-post* decisions studied are simple and do not require proactive management of the damage after the incident. For example, Abbring et al. (2008) and Gramig et al. (2005) formulate *ex-post* moral hazard as a binary decision variable, such as report vs. not report or disclose vs. not disclose. In health insurance, the concern is the abuse of healthcare insurance after an illness. The objective is to induce consumers to adopt a healthy lifestyle to prevent illness (Bogetic and Heffley 1993). Instead of internalizing

the prevention and mitigation decisions with insurance, this literature focuses on incentive plans to alter the lifestyles of the insured so as to reduce the *ex-post* costs (Heffley and Miceli 1998).

Here, we do not consider incentive plans, as they are relatively uncommon in cyber insurance. Our analysis of risk mitigation and risk prevention in cybersecurity adopts the self-insurance (to reduce the severity of loss in a security incident) and self-protection (to reduce the probability of a security incident) concepts proposed by Ehrlich and Becker (1972). The point of departure here is that the risk-mitigation decisions are made *ex-post*, i.e., after the security breach incident, instead of *ex-ante*.

2.2 Management of Cybersecurity

Cybersecurity management encompasses a large number of technical and managerial measures. The IT security risk management framework is commonly used in many organizations. In this framework, countermeasures are prioritized on the basis of which threats or risks are ranked the most dangerous (Loch et al. 1992). The protection effort should not exceed what is justifiable by the associated costs and losses (Gordon and Loeb 2002). In other words, protection does not need to be aimed at preventing all security breaches. Instead, firms typically operate under the notion of "acceptable" risk, where any decisions about reducing risks recognize a degree of residual risk that the firm is willing to accept (Whitman and Mattord 2012).

Recent studies have focused on the economic incentives for managing information security. This stream of research examines issues related to breach prevention (Cavusogluet al. 2005, Mookerjee et al. 2011), risk transfer (Zhao et al. 2013, Hui et al. 2013), security risk disclosure and realization (Gordon et al. 2006, Wang et al. 2013), sharing of cybersecurity related information (Gordon, Loeb and Lucyshyn 2003), mandatory information security standards (Lee et al. 2016), contracting information security (Lee et al. 2013, Hui et al. 2019), intrusion detection and response (Yue and Cakanyildirim 2007), portfolio approaches to examining the aggregate values of different sets of countermeasures (Kumar et al. 2008), a value-at-risk (VaR) approach for information security investment (Wang et al. 2008), wait-and-see approach to risk prevention (Bohme and Moore 2009, Elliott et al. 2016), diffusion and disclosure of attacks

(Mitra and Ransbotham 2015), and software liability and vulnerability (August and Tunca 2011). However, these studies do not consider post-breach risk mitigation as an aspect of cybersecurity risk management. Our study extends this literature by studying the interplay between cybersecurity risk prevention, mitigation, and transfer and how they interact to affect the overall risk borne by the insured firm.

3. Model and Analysis

Consider a two-stage model in which the firm makes an investment to prevent a cybersecurity breach at $t = 0$. The investment is in risk prevention measures such as technical controls, security policy deployment, and awareness training. An investment s gives the firm risk prevention effectiveness $q(s)$, where $0 < q(s) < 1$. A higher risk prevention effectiveness lowers the breach probability, denoted as $[1 - q(s)]$ (Gordon and Loeb 2002), where $q'(s) > 0$ and $q''(s) < 0$, i.e., there is diminishing return to risk prevention investment. Realistically, it is difficult if not impossible to achieve perfect security. As the level of security increases, the effort needed to raise security further increases disproportionally.

If a breach such as unauthorized access or distributed denial of service attacks occurs, an *unmitigated* loss will be incurred. The firm then moves into the post-breach stage, $t = 1$, and will engage in mitigation spending r on activities such as incident response and disaster recovery, which reduce the loss arising from the security breach. Any remaining loss after this stage is called *mitigated* loss. We assume that the decision timeline spans one financial year, which is consistent with the typical annual budgeting cycle for cybersecurity risk management (PwC 2014). Figure 1 illustrates the decision timeline.

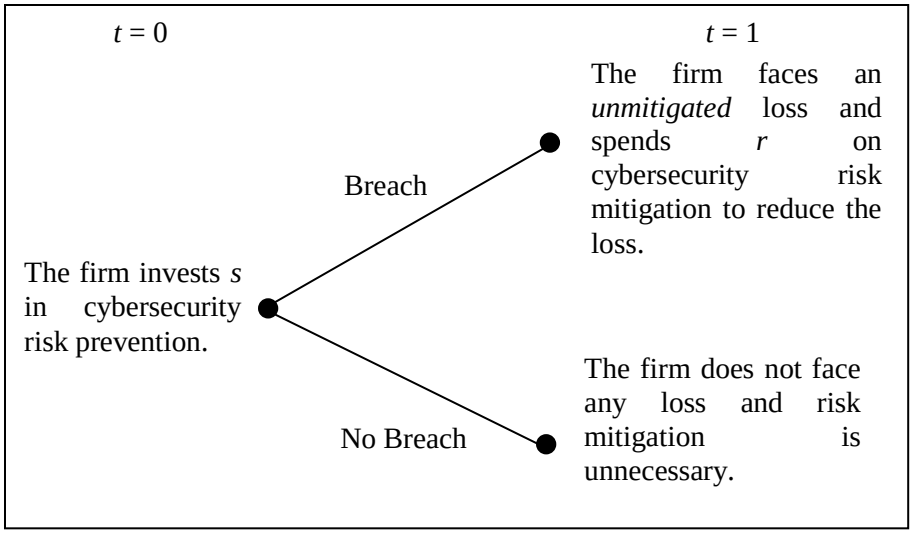


Figure 1. Decision Timeline

Conditional on breach occurrence, the mitigated loss suffered by the firm is

$$[1 - m(r)]L,$$

where L is a random variable that denotes the unmitigated loss and $m(r)$ denotes the effectiveness of post-breach mitigation spending, r, where $0 < m(r) < 1$, $m'(r) > 0$, and $m''(r) < 0$. Here again, risk mitigation is subject to diminishing returns for the same reason as risk prevention. Throughout this paper, we use upper case letters to denote random variables and cumulative probability distributions. We use lowercase letters for other variables and functions.

Our definition of cybersecurity risk, which considers both the likelihood of an incident and the severity of the incident, is consistent with the definitions in the literature (Kaplan and Garrick 1981). Similar to Gordon and Loeb (2002), we assume that investment in preventive measures reduces the likelihood of a breach. In contrast, risk mitigation investment limits the size of the breach severity (i.e., losses).

To facilitate subsequent analysis, we assume $q(s)$ and $m(r)$ have the following forms:

$$q(s) = 1 - e^{-k_s s} \text{ and}$$

$$m(r) = 1 - e^{-k_r r},$$

where parameters k_s and k_r dictate the concavity of the functions. Larger values of these parameters represent greater degrees of concavity, as shown in Figure 2. In Appendix J, we prove that except for

Proposition 4, which requires a more general interpretation, all of our key results continue to hold without relying on the functional forms of $q(s)$ and $m(r)$. Table 1 summarizes the notation used in our analysis.

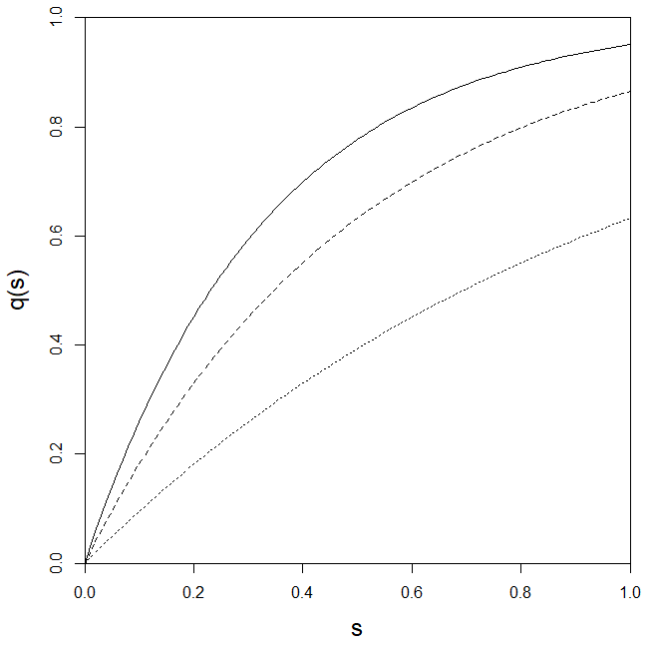


Figure 2. $q(s)$ under different values of k_s (Dot: $k_s = 1$, Dash: $k_s = 2$, Solid: $k_s = 3$)

Table 1. Notation Table

Symbol	Description
r	Risk mitigation spending
s	Risk prevention investment
$q(s)$	Risk prevention effectiveness
$m(r)$	Risk mitigation effectiveness on unmitigated loss
w_0	Initial wealth at the beginning of $t = 0$
w_1	Wealth at the end of $t = 1$
U	Utility
U^*	Utility after solving for r at $t = 1$ in backward induction
U^{**}	Utility after solving for s at $t = 0$ in backward induction
L	Unmitigated loss
p	Price of cyber insurance
k	Size of claim
β	Scope of insurance coverage
δ	Depth of insurance coverage/One minus the coinsurance rate
c	Subscript for the cyber insurance model
b	Subscript for the base model

3.1 Base Model

In this subsection, we consider a base case where the firm addresses security risks without using cyber insurance. Assuming risk neutrality, the firm's expected utility is

$$E[U] = w_0 - s - [1 - q(s)]E\{r + [1 - m(r)]L\},$$

where w_0 denotes the firm's initial wealth. The firm's objective is to maximize its final utility.

We solve the problem backwards. At $t = 1$, the firm suffers no damage if there is no breach. The firm's wealth at the end of $t = 1$ remains the same as that at the end of $t = 0$, i.e., $w_1 = w_0 - s$. If there is an incident, however, the true value of the unmitigated loss is revealed; the firm learns that $L = \ell$. After post-breach mitigation measures, the firm eventually suffers a mitigated loss of $[1 - m(r)]\ell$. In this study, we call this loss *risk acceptance*. Thus, given any s at $t = 0$, the firm's wealth after the cybersecurity incident at $t = 1$ is

$$w_1 = w_0 - s - r - [1 - m(r)]\ell.$$

Compared with the case of no breach, where $w_1 = w_0 - s$, we see that the total impact of a breach at the end of $t = 1$, denoted as Δw, is $\Delta w = r + [1 - m(r)]\ell$. In other words, the impact of a breach to the firm includes the mitigated loss and the spending on mitigation.

Now, when a breach occurs, the firm chooses r to maximize w_1. It will increase the post-breach risk mitigation spending until the additional dollar spent yields an exact dollar worth of benefit. This optimal level can be obtained by solving the first-order condition:

$$\frac{dw_1}{dr} = -1 + m'(r)\ell = 0.$$

In the above expression, the first term represents the marginal cost of risk mitigation spending. The second term is the marginal benefit of risk mitigation. The first-order condition can be rewritten as

$$m'(r) = \frac{1}{\ell}. \quad (1)$$

The second-order condition is satisfied as $m''(r) < 0$. Solving for Equation (1) allows the firm to determine the optimal level of spending on risk mitigation based on s and ℓ. We denote this optimal level of risk mitigation spending as $r^*(\ell)$. Substituting $m(r) = 1 - e^{-k_r r}$ into Equation (1) yields

$$r_b{}^*(\ell) = \frac{1}{k_r}\ln(k_r\ell), \quad (2)$$

where the subscript b denotes the base case. The optimal risk mitigation spending increases with the unmitigated loss and is independent of the risk prevention investment s, and

$$w_1{}^* = w_0 - s - \frac{1}{k_r}[1 + \ln(k_r \ell)].$$

Moving backwards, at $t = 0$, the actual value of ℓ is not yet realized. So, at $t = 0$, the firm has to make decisions based on the expected $r_b{}^*(L)$, which is a function of a random variable, L:

$$E[U^*] = q(s)(w_0 - s) + [1 - q(s)]E\left\{w_0 - s - \frac{1}{k_r}[1 + \ln(k_r L)]\right\}. \quad (3)$$

The first-order condition is

$$\frac{\partial E[U^*]}{\partial s} = -1 + q'(s)E\left\{\frac{1}{k_r}[1 + \ln(k_r L)]\right\} = 0, \text{ or} \quad (4)$$

$$s_b{}^* = \frac{1}{k_s}\ln\left\{\frac{k_s}{k_r}E[1 + \ln(k_r L)]\right\}. \quad (5)$$

The second-order condition is

$$q''(s)E\left\{\frac{1}{k_r}[1 + \ln(k_r L)]\right\} < 0, \quad (6)$$

because $q''(s) < 0$. Hence, the expected risk prevention effectiveness is

$$q(s_b{}^*) = 1 - e^{-k_s s_b^*} = 1 - \frac{k_r}{k_s}\frac{1}{E[1+\ln(k_r L)]}, \quad (7)$$

and the expected welfare change (compared to the case of no incident) at $t = 1$ evaluated at $t = 0$ is

$$E[\Delta W_1{}^{**}] = [1 - q(s_b{}^*)]E[W_1{}^{**} - (w_0 - s_b^*)] = \frac{k_r}{k_s}\frac{1}{E[1+\ln(k_r L)]} \times \frac{1}{k_r}E[1 + \ln(k_r L)] = \frac{1}{k_s}. \quad (8)$$

Note that the welfare change (i.e., the overall effect of the incident including the risk mitigation spending) in the expectation function above is a random variable because at the time of the evaluation of the expectation ($t = 0$) the incident has not yet happened.The equilibrium expected post-breach risk mitigation spending is

$$[1 - q(s_b{}^*)]E[\, r_b{}^*(L)] = \frac{1}{k_s}\frac{E[\ln(k_r L)]}{E[1+\ln(k_r L)]}. \quad (9)$$

We refer to the final loss suffered by the firm as the eventual cybersecurity risk the firm chooses to accept. The equilibrium expected risk acceptance level is

$$[1 - q(s_b{}^*)]E\left[\left\{1 - m\left(\, r_b{}^*(L)\right)\right\}L\right] = \frac{1}{k_s}\frac{1}{E[1+\ln(k_r L)]}. \quad (10)$$

The equilibrium expected utility is

$$E[U^{**}] = w_0 - {s_b}^* - [1 - q({s_b}^*)]E\left\{\frac{1}{k_r}[1 + \ln(k_r L)]\right\}. \quad (11)$$

Hence,

$$E[U^{**}] = w_0 - \frac{1}{k_s}\left(1 + \ln\left\{\frac{k_s}{k_r}E[1 + \ln(k_r L)]\right\}\right). \quad (12)$$

Proposition 1 summarizes the outcomes of the base model.

Proposition 1. *The equilibrium of the base model is characterized as follows.*

(a) Expected risk prevention investment ${s_b}^* = \frac{1}{k_s}\ln\left\{\frac{k_s}{k_r}E[1 + \ln(k_r L)]\right\}$.

(b) Expected risk prevention effectiveness $q({s_b}^*) = 1 - \frac{k_r}{k_s}\frac{1}{E[1+\ln(k_r L)]}$.

(c) Expected risk mitigation spending for a given breach ${r_b}^*(\ell) = \frac{1}{k_r}\ln(k_r \ell)$.

(d) Expected risk mitigation spending $[1 - q({s_b}^*)]E[\,{r_b}^*(L)] = \frac{1}{k_s}\frac{E[\ln(k_r L)]}{E[1+\ln(k_r L)]}$.

(e) Expected risk acceptance $[1 - q({s_b}^*)]E\left[\left\{1 - m\left({r_b}^*(L)\right)\right\}L\right] = \frac{1}{k_s}\frac{1}{E[1+\ln(k_r L)]}$.

(f) Expected firm utility $E[U^{**}] = w_0 - \frac{1}{k_s}\left(1 + \ln\left\{\frac{k_s}{k_r}E[1 + \ln(k_r L)]\right\}\right)$.

The equilibrium outcomes listed in Proposition 1 serve as a baseline for our study of the effects of cyber insurance.

3.2 Cyber Insurance Model

We now consider the case where cyber insurance is adopted as one component of the firm's risk management strategy (Hurtaud et al. 2015, Stark and Fontaine 2015).[4] Specifically, we examine how it affects the firm's risk prevention and post-breach risk mitigation actions.

For simplicity, we assume perfect competition for the supply of cyber insurance such that the price is exogenous. We also assume that a cyber insurance market exists, meaning it creates sufficient value via

[4] Cyber insurance coverage may include loss of revenue from security breaches, hiring a forensic or crisis management firm, legal fees, breach notification expenses, and third-party liability and credit monitoring services for customers (Higgins 2014; Perlroth and Harris 2014).

economies of scale and effective risk pooling. In the following analysis, we focus on the demand side of cyber insurance. Figure 3 illustrates the timeline for the cyber insurance model.

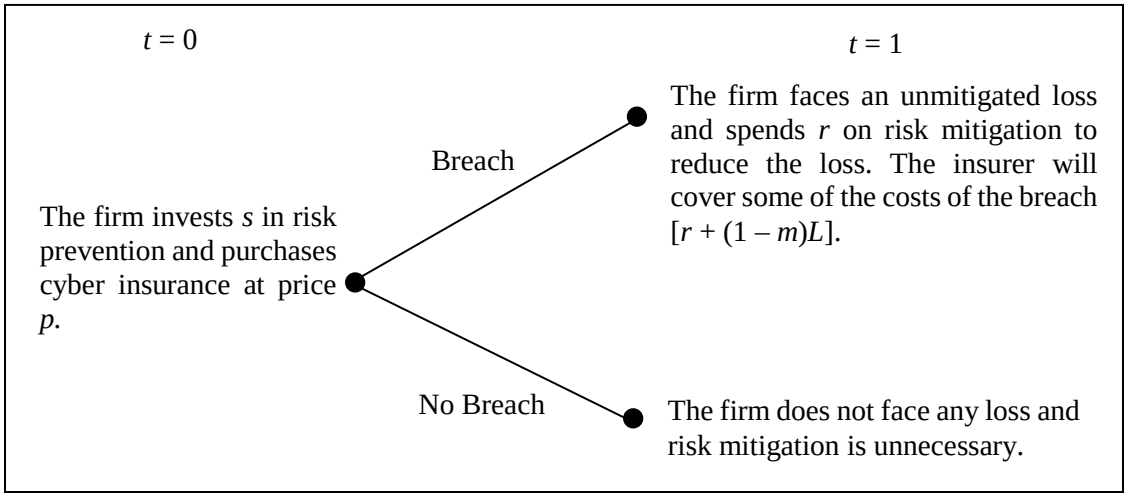


Figure 3. Cyber Insurance Model

After the firm purchases cyber insurance by paying price p at $t = 0$, the basic premise is that the insurance will cover the mitigation spending and some of the mitigated loss at $t = 1$ when a security breach occurs. With cyber insurance, the firm's expected utility at $t = 0$ is

$$E_g[U] = w_0 - s - p - [1 - q(s)]E_g[r + [1 - m(r)]L - k], \tag{13}$$

where k denotes the insurance coverage, which is a function of the cost of the breach, say, x, covered by the cyber insurance, i.e., $k = k(x)$. The function $k(x)$ is typically a linear or piecewise linear function.[5] We assume $k(x) = \delta x$, where $0 < \delta \leq 1$. Following Feldman et al. (1997), we call δ the "depth" of coverage.

Here, x denotes the firm's change in wealth due to the breach, which comprises mitigation spending, r, and the types of loss covered by the insurance policy. The loss covered is typically less than the mitigated loss $[1 - m(r)]\ell$. For example, some cyber insurance products do not cover reputation damage (Hurtaud

[5] For example, for full coverage (Bolot and Lelarge 2008; Hofmann 2005), $k(x) = x$. For a simple deductible schedule (Doherty and Schlesinger 1983; Pashigian et al. 1966; Gould 1969), $k(x) = (x - d)\mathbb{I}\{x > d\}$, where d is the deductible and $\mathbb{I}$ is the indicator function. For co-insurance (Crew 1969, Phelps and Newhouse 1974), $k(x) = \delta x$, where δ represents the proportion of the loss borne by the insurer. For simplicity, we assume $k(x) = \delta x$ and $0 < \delta \leq 1$, which encompasses both full coverage and co-insurance. Our results do not apply to deductible insurance.

et al. 2015). We refer to the types of mitigated loss covered as the *scope* of coverage (Zoidze et al. 2013, van der Wees et al. 2016)[6] and denote it as β, where $0 < \beta < 1$. In general, a narrow scope (i.e., small β) means more exclusions in the cyber insurance contract. Taken together, $k = \delta\{r + \beta[1 - m(r)]\ell\}$.

We again solve the problem by backward induction. At $t = 1$, the potential loss unfolds. The firm will maximize

$$w_1 = w_0 - s - p - r - [1 - m(r)]\ell + \delta(r + \beta[1 - m(r)]\ell).$$

The first derivative with respect to r can be simplified to

$$\frac{dw_1}{dr} = -(1 - \delta) + (1 - \beta\delta)m'(r)\ell. \tag{14}$$

The first term represents the marginal cost of risk mitigation spending. The second term is the marginal benefit of risk mitigation (i.e., loss reduction). Comparing this model with the base case, the marginal cost of risk mitigation is reduced from 1 to $1 - \delta$, and the marginal benefit of risk mitigation is reduced from $m'(r)\ell$ to $(1 - \beta\delta)m'(r)\ell$. Hence, relative to the base case, the reduction in marginal cost is greater than the reduction in marginal benefit.

The first-order condition can be simplified to

$$m'(r) = \frac{1-\delta}{(1-\beta\delta)\ell}. \tag{15}$$

We denote the optimal risk mitigation spending at this stage as $r_c^*(\ell)$. We use the subscript c to denote the cyber insurance model. With $m(r) = 1 - e^{-k_r r}$, it can be shown that

$$r_c^*(\ell) = \frac{1}{k_r} \ln\left(\frac{1-\beta\delta}{1-\delta} k_r \ell\right). \tag{16}$$

The only difference between Equation (16) and Equation (2) is the presence of the factor $\frac{1-\beta\delta}{1-\delta}$ in the natural log function of Equation (16). As $\frac{1-\beta\delta}{1-\delta} > 1$, Equation (16) is larger than Equation (2).

[6] Note that the different dimensions of insurance coverage have various names in the literature. For example, in Feldman et al. (1997), "breadth" is used to refer to the number of types of services covered in an insurance policy and, like us, "depth" is used to refer to the proposition of the costs covered by the insurance. However, Soors et al. (2010) refer to the number of types of services covered as "depth" and the proportion of the costs covered as "height."

Proposition 2. *Compared with the base model, the cyber insurance model increases the optimal (ex-post) risk mitigation spending r^* when a security incident occurs.*

Proposition 2 states that cyber insurance tends to encourage risk mitigation spending by reducing the marginal cost of risk mitigation: a proportion of every dollar spent on risk mitigation is now borne by the insurer. Although the marginal benefit of risk mitigation is also reduced because some of the benefits of risk mitigation are now shared by the insurer, incomplete coverage in terms of scope (i.e., $\beta < 1$) ensures that the insurer's share of the benefits is smaller than its share (δ) of the covered risk types. As the marginal cost of risk mitigation is reduced to a greater extent than the marginal benefit of risk mitigation, there is an overall increase in the *ex-post* risk mitigation spending. This finding is consistent with observations in the health insurance context, where policy holders often spend more on health services than non-holders (Pauly 1968).

With Equation (16), we can compute the firm's wealth at $t = 1$ in case of a security breach as

$$w_1{}^* = w_0 - s - p - \frac{1}{k_r}(1-\delta)\left[1 + \ln\left(\frac{1-\beta\delta}{1-\delta}k_r\ell\right)\right].$$

Solving the problem backwards, the firm's expected utility at $t = 0$ is

$$E[U^*] = w_0 - s - p - [1 - q(s)]E\left\{\frac{1}{k_r}(1-\delta)\left[1 + \ln\left(\frac{1-\beta\delta}{1-\delta}k_rL\right)\right]\right\}. \quad (17)$$

Differentiating with respect to s,

$$\frac{\partial E[U^*]}{\partial s} = -1 + q'(s)E\left[\frac{1}{k_r}(1-\delta)\left[1 + \ln\left(\frac{1-\beta\delta}{1-\delta}k_rL\right)\right]\right] = 0, \quad (18)$$

which gives

$$s_c{}^* = \frac{1}{k_s}\ln\left\{\frac{k_s}{k_r}(1-\delta)E\left[1 + \ln\left(\frac{1-\beta\delta}{1-\delta}k_rL\right)\right]\right\}. \quad (19)$$

Equation (19) is similar to Equation (5), except that the term related to the optimal risk mitigation spending is multiplied by a factor of $\frac{1-\beta\delta}{1-\delta}$, and the size of the quantity in the outer natural logarithm function is scaled down by a factor of $(1-\delta)$. Appendix C explains why the risk prevention investment at $t = 0$ is decreased, i.e., $s_c{}^* < s_e{}^*$. This reflects the classic moral hazard problem in insurance and is consistent with Gordon, Loeb, and Sohail (2003).

Proposition 3. *Compared with the base model, the cyber insurance model decreases risk prevention, i.e.,* ${s_c}^* < {s_b}^*$.

The equilibrium risk prevention effectiveness is therefore

$$q({s_c}^*) = 1 - \frac{k_r}{k_s}\frac{1}{1-\delta}\frac{1}{1+E\left[\ln\left(\frac{1-\beta\delta}{1-\delta}k_r L\right)\right]},$$

and the expected welfare change at $t = 1$ is

$$E[\Delta {W_1}^{**}] = \frac{k_r}{k_s}\frac{1}{1-\delta}\frac{1}{1+E\left[\ln\left(\frac{1-\beta\delta}{1-\delta}k_r L\right)\right]} \times \frac{1}{k_r}(1-\delta)\left[1+\ln\left(\frac{1-\beta\delta}{1-\delta}k_r L\right)\right] = \frac{1}{k_s}. \quad (20)$$

As Equation (8) is the same as Equation (20), we have the following lemma.

Lemma 1. *Compared to the base model, the cyber insurance model does not affect the expected welfare change at t = 1.*

Lemma 1 suggests that the firm is not really expected to be better off with cyber insurance at $t = 1$ than without it. As explained in Appendix J, this result depends on the functional form of $q(s)$ (but not $m(r)$). For other functional forms of $q(s)$, Lemma 1 highlights the ambivalent welfare effect of purchasing cyber insurance. Although cyber insurance can reduce the overall cost of a breach, the firm becomes less motivated to invest in risk prevention, which moderates the welfare benefit of cyber insurance.

Because of Lemma 1, the firm's decision to buy cyber insurance depends only on its equilibrium wealth at the end of $t = 0$. Appendix E proves the following proposition.

Proposition 4. *If the price of cyber insurance is smaller than the decrease in risk prevention investment in the base model, i.e.,* $p < s_b^* - s_c^*$*, the firm will buy cyber insurance.*

As Proposition 4 depends on Lemma 1, it does not apply to other functional forms of $q(s)$. However, the general interpretation of Proposition 4 is that when the expected welfare effects of cyber insurance are small, the firm's decision to purchase cyber insurance can be simplified to comparing the cost of the cyber insurance and the reduction in optimal risk prevention investment. In Appendix J, we show that the precise condition for the firm's purchase of cyber insurance is

$$p < s_b^* - s_c^* + \frac{1-q(s_b^*)}{q'(s_b^*)} - \frac{1-q(s_c^*)}{q'(s_c^*)}.$$

The equilibrium expected risk mitigation spending is

$$[1 - q(s_c{}^*)]E[\, r_c^*(L)] = \frac{1}{k_s}\frac{1}{1-\delta}\frac{E\left[\ln\left(\frac{1-\beta\delta}{1-\delta}k_r L\right)\right]}{1+E\left[\ln\left(\frac{1-\beta\delta}{1-\delta}k_r L\right)\right]}. \quad (21)$$

Appendix F proves the following corollary.

Corollary 1. *Compared with the base model, the cyber insurance model increases expected risk mitigation spending.*

Corollary 1 is not surprising because both the mitigation spending per incident and the probability of a breach are increased (Propositions 2 and 3). Together with Proposition 3, the corollary points to the tendency for cyber insurance to re-align resources from risk prevention to risk mitigation, which, incidentally, has been a recent recommendation by cybersecurity practitioners (Noel 2017).

The equilibrium expected risk acceptance with cyber insurance is

$$[1 - q(s_c{}^*)]E\left[\left\{1 - m\left(\, r_c^*(L)\right)\right\}L\right] = \frac{1}{k_s}\frac{1}{1-\beta\delta}\frac{1}{1+E\left[\ln\left(\frac{1-\beta\delta}{1-\delta}k_r L\right)\right]}. \quad (22)$$

Appendix G proves the following proposition.

Proposition 5. *Compared with the base model, the cyber insurance model decreases expected risk acceptance if its scope, β, is sufficiently small.*

Specifically, Proposition 5 holds if

$$\beta < \frac{1}{\delta} - \frac{E[1+\ln(k_r L)]}{\delta W\left(\frac{E[1+\ln(k_r L)]e^{E[1+\ln(k_r L)]}}{1-\delta}\right)}.^{7}$$

For example, if $E[\ln(k_r L)] = 1$, the regions where cyber insurance increases or decreases risk acceptance is as depicted in Figure 4.

[7] The W function is simply the inverse of $f(x) = xe^x$.

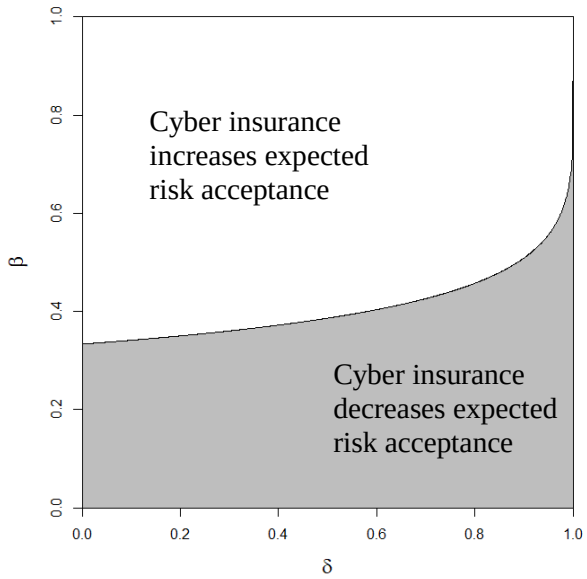
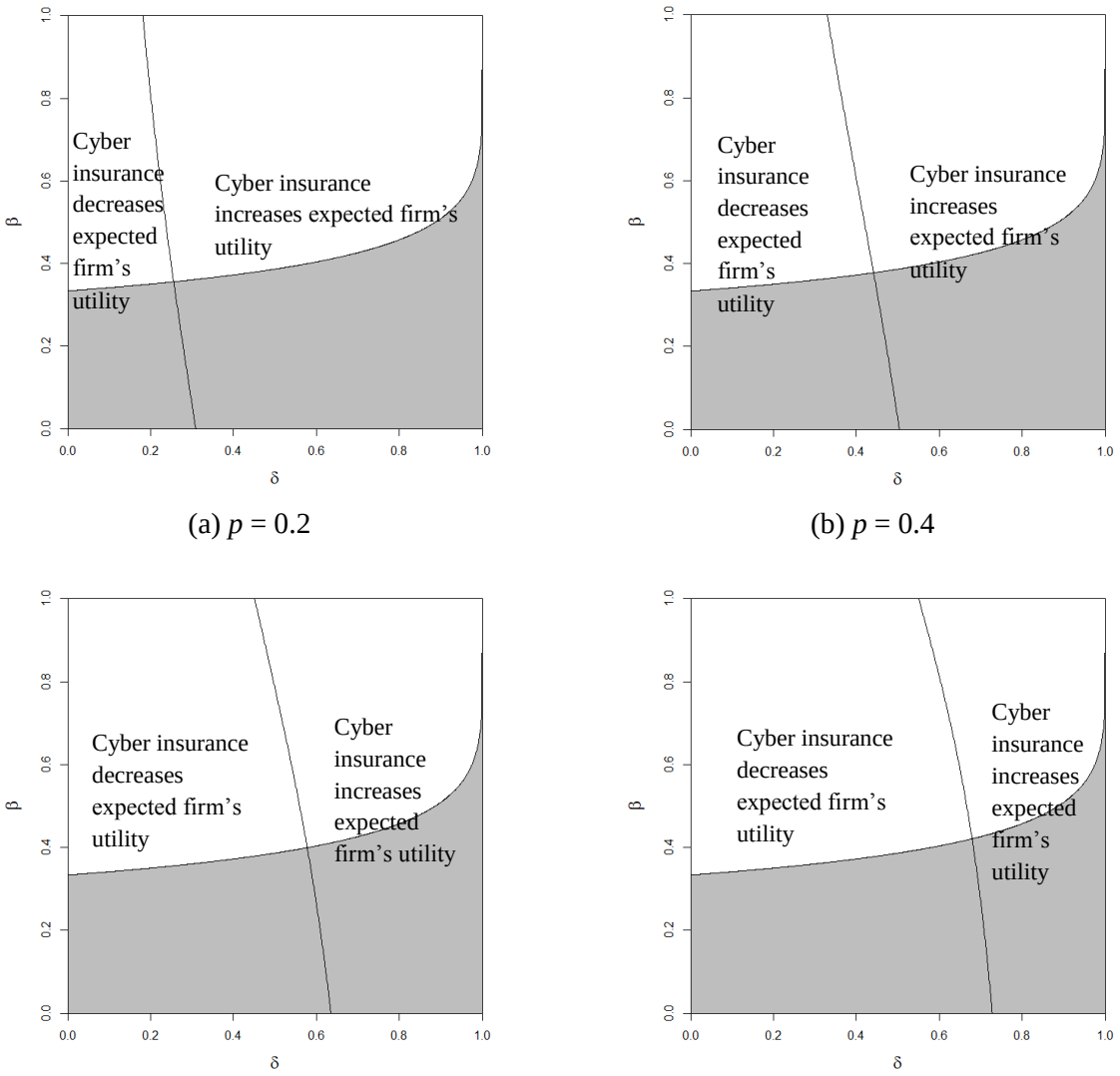


Figure 4. Effects of Cyber Insurance on Risk Acceptance ($E[\ln(k_r L)] = 1$)

To complete the analysis, we substitute s_c^* into Equation (17) to obtain the firm's expected utility:

$$E[U^{**}] = w_0 - p - \frac{1}{k_s} - \frac{1}{k_s}\ln\left\{\frac{k_s}{k_r}(1-\delta)E\left[1 + \ln\left(\frac{1-\beta\delta}{1-\delta}k_r L\right)\right]\right\}. \quad (23)$$

We compare the above equation with Equation (12), and Figures 5(a) to 5(d) show the numerical results for cases of cyber insurance at different levels of p for $E[\ln(k_r L)] = 1$ and $k_s = 1$. On the left of the solid black lines are areas corresponding to cyber insurance decreasing the firm's expected utility and the right of the black lines are areas corresponding to cyber insurance increasing the firm's expected utility. Note that the grey areas in Figure 5 correspond to the grey areas in Figure 4. At the lower right corner of the figures, where the scope is reasonably low and the depth is reasonably high, the firm can accept a smaller risk while achieving higher utility.



(a) p = 0.2

(b) p = 0.4

(c) p = 0.6

(d) p = 0.8

Figure 5. Effects of Cyber Insurance on Expected Firm's Utility ($E[\ln(k_r L)] = 1$ and $k_s = 1$)

Overall, our analysis suggests that cyber insurance encourages risk mitigation for a given level of risk prevention investment because the insurer bears some of the costs (Proposition 2). However, the level of risk prevention investment is decreased because the firm becomes less concerned about the consequences of a security breach (Proposition 3). The overall effect is an increase in expected risk mitigation spending (Corollory 1). From a cybersecurity perspective, whether the expected level of risk acceptance is decreased depends on the cyber insurance's scope and depth of coverage. Cyber insurance is more likely to decrease

risk acceptance if the scope of coverage is small or depth of coverage is large (Proposition 5). Our analysis also shows that the firm will purchase cyber insurance if it is not too costly (Proposition 4).

3.3 Comparative Statics

We perform comparative statics with respect to β and δ to investigate how cyber insurance affects equilibrium expected risk prevention, risk mitigation, risk acceptance, and the insured firm's utility. The derivations are available in Appendix H.

Table 2. Comparative Statics

	$\frac{\partial}{\partial \beta}$	$\frac{\partial}{\partial \delta}$
Equilibrium Expected Risk Prevention Investment, s_c^*	negative	negative
Equilibrium Expected Risk Prevention Effectiveness, $q(s_c^*)$	negative	negative
Expected Risk Mitigation Spending for a Given Breach, $r_c^*(\ell)$	negative	positive
Equilibrium Expected Risk Mitigation Spending, $[1 - q(s_c{}^*)]E[\, r_c^*(L)]$	negative	positive
Equilibrium Expected Risk Acceptance, $[1 - q(s_c{}^*)]E\big[\{1 - m\big(\, r_c^*(L)\big)\}L\big]$	positive	positive or negative
Equilibrium Expected Firm's Utility, $w_0 - s_c{}^* - p - [1 - q(s_c{}^*)]\{(1-\delta)\, r_c^*(L) + (1-\beta\delta)\big[1 - m\big(\, r_c^*(L)\big)\big]L\}$	positive	positive

The comparative statics provide us with more in-depth insights into the mechanism that drives our propositions. Although β and δ affect expected risk prevention in the same direction, they affect risk mitigation in opposite directions (highlighted in grey in Table 2). A positive relationship between δ and risk mitigation spending is not surprising. A greater depth in insurance coverage means that the insurer bears more of the risk mitigation spending, decreasing the firm's marginal cost of risk mitigation and thus encouraging risk mitigation spending. A less intuitive result is that a small β actually favors risk mitigation spending for a given incident. This occurs because a small β ensures that the marginal benefit of risk mitigation is not reduced to a degree that significantly cancels out the effects of the reduced marginal cost of risk mitigation. Otherwise, the expected risk acceptance will increase.

4. Theoretical Contribution and Practical Implications

4.1 Theoretical Contribution

Our study makes two novel theoretical contributions to the literature. First, we demonstrate that the notion of insurance aggravating *ex-ante* moral hazard has a somewhat different meaning in the context of cyber insurance. Instead of promoting shirking, as seen in traditional insurance, cyber insurance facilitates the reallocation of resources from risk prevention to risk mitigation, where the effect of *ex-ante* moral hazard may be offset by more *ex-post* effort. This reallocation of resources may lead to a preferred outcome of achieving greater firm utility and a lower level of accepted risk. Although prior studies have considered the interplay between cyber insurance and risk prevention, this is the first study to consider *ex-post* risk mitigation.

Second, we show that the firm is better off when the insurance coverage is sufficiently deep and the scope is sufficiently narrow. This contradicts the typical wisdom that deep coverage exacerbates the moral hazard problem. Compared to the case with no cyber insurance, deep cyber insurance coverage encourages *ex-post* effort investment because it reduces the marginal benefit of risk mitigation less than marginal cost, which can be beneficial in reducing the accepted risk.[8] Narrower coverage puts pressure on the firm to exert appropriate risk prevention investment. This nuanced effect of cyber insurance ultimately helps incentivize firms to take actions that improve their welfare and reduce cybersecurity risk.

4.2 Practical Implications

From the managerial standpoint, our study indicates the importance of having a holistic view when managing cybersecurity risks. Effective cybersecurity risk management is rooted in the seamless integration of different risk management measures. As shown in our analysis, the optimal use of cyber insurance policies requires a balanced adjustment of risk prevention investment and risk mitigation effort.

Neglecting post-breach risk mitigation may lead to dire consequences, yet it is an area that many firms often overlook. According to a worldwide survey conducted by the Ponemon Institute and IBM in

[8] In the healthcare literature, this effect is referred as *ex-post* moral hazard (Grignon et al. 2018, Zweifel and Manning 2000).

2018, 77 percent of firms lack consistent organizational incident response plans.[9] Anecdotal evidence indicates that improper incident response could be detrimental to firms. For example, poor incident response led to one of the largest data breach incidents in Singapore in 2018 (Tham and Baharudin 2018). In other cases, such as the Target breach in 2013, the public relations crisis that followed after the mishandling of the breach incident led to a major reputation loss for Target (Temin 2013).

With cyber insurance serving as an important guarantor for post-breach losses, the effect of *ex-post* risk mitigation is amplified. Many cybersecurity insurers require breached firms to immediately notify them about the nature of the breach incidents such that further actions can be planned.[10] Some insurance policies also mandate which outside risk mitigation agency (e.g., forensic investigator, public relations agency, legal counsel, etc.) a firm can engage after a security breach incident (FERMA 2018, OECD 2017). According to KPMG, the emerging industry trend is that clients are pushing insurers to offer broad-based, post-breach solutions instead of just an insurance product (Merrey et al. 2017). Our results illustrate the crucial interplay between cyber insurance and risk mitigation and prevention.

From the policy makers' perspective, although cyber insurance has long been regarded as a potentially important tool for managing firms' cybersecurity risks, there is a lack of quality actuarial data. Recently, the National Association of Insurance Commissioners (NAIC) in the United States mandated insurers who offer cybersecurity and identity theft policies to report critical policy-related information in their annual financial reports.[11] Such information will help to provide the market with the required actuarial data for fair policy underwriting. Although the insurers may not write a detailed policy to cover every type of cybersecurity risk, our analysis shows that covering certain types of risk comprehensively may effectively reduce firms' cybersecurity risks.

[9] Source https://newsroom.ibm.com/2018-03-14-IBM-Study-Responding-to-Cybersecurity-Incidents-Still-a-Major-Challenge-for-Businesses

[10] For example, XL Catlin (now acquired by AXA) presented a cyber claims road map to clients in the event of a cybersecurity breach https://axaxl.com/en-ca/insurance/dp/products/-/media/3811bf346817496fae623916cc04ca13.ashx

[11] For example, the number of claims reported, direct premiums written and earned, and direct losses paid and incurred.

5. Conclusion

We analyze a two-stage model that incorporates risk prevention, risk mitigation, and risk transfer via cyber insurance as a part of firms' risk control strategies. Specifically, we study how cyber insurance affects risk prevention and risk mitigation and its security and welfare implications. More importantly, we show how cyber insurance can be better designed to complement existing cybersecurity risk management strategies.

Our results point to several future research directions. First, our study has assumed that the firm is risk-neutral. In reality, risk aversion may affect the utility-maximizing optimal amount of financial resources that a firm needs to be put aside for risk mitigation. Second, it would be interesting to analyze the sensitivity of our results to a deductible cyber insurance schedule. Finally, future research should consider the pricing of cyber insurance and the competitive structure of the cyber insurance market.

References

Abbring, J. H., P. A. Chiappori, and T. Zavadil. 2008. Better safe than sorry? Ex ante and ex post moral hazard in dynamic insurance data. Discussion Paper No. 08-075/3, Tinbergen Institute.

Arrow, K. J. 1963. "Uncertainty and the Welfare Economics of Medical Care." *American Economic Review* 53: 941-973.

Bandyopadhyay, Tridib, Vijay S. Mookerjee, and Ram C. Rao. 2008. "Why IT Managers Don't Go for Cyber-Insurance Products." *Communications of ACM* 52 11: 68-73.

Bodin, Lawrence D., Lawrence A. Gordon, Martin P. Loeb, and Aluna Wang. 2018. "Cybersecurity Insurance and Risk-Sharing." *Journal of Accounting and Public Policy* 37: 527-544.

Bogetic, Zeljko, and Dennis Heffley. 1993. Reforming health care: A case for stay well health insurance. Policy, Research working papers no. WPS 1181., Washington, DC: World Bank.

Bohme, Rainer. 2005. "Cyber-Insurance Revisited." *Workshop on the Economics of Information Security (WEIS)*, Cambridge, MA.

Bohme, Rainer, and Gaurav Kataria. 2006. "Models and Measures for Correlation in Cyber-Insurance." *Workshop on the Economics of Information Security (WEIS)*, Cambridge, UK.

Bohme, Rainer, and Tyler Moore. 2009. "The Iterated Weakest Link: A Model of Adaptive Security Investment." *Workshop on the Economics of Information Security (WEIS)*, London, UK.

Bolot, Jean, and Marc Lelarge. 2008. "Cyber Insurance as an Incentive for Internet Security." *The Seventh Workshop on Economics of Information Security*. Hanover, NH.

Burrows, Jim. 2017. “Escaping Dark Age Cybersecurity Thinking.” Medium.com. 1 Feb. https://medium.com/@brons/escaping-dark-age-cybersecurity-thinking-3e7b0c74bda8.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 2005. “The Value of Intrusion Detection Systems in Information Technology Security Architecture.” *Information Systems Research* 16 (1): 28-46.

Crew, Michael. 1969. “Coinsurance and the Welfare Economics of Medical Care.” *American Economic Review* 59 (5): 906-908.

Doherty, Neil A., and Harris Schlesinger. 1983. “The Optimal Deductible for an Insurance Policy When Initial Wealth is Random.” *The Journal of Business* 56 (4): 555-565.

Ehrlich, Isaac, and Gary S. Becker. 1972. “Market Insurance, Self-insurance, and Self-protection.” *Journal of Political Economy* 80 (4): 623-648.

Elliott, Karen, Fabio Massacci, and Julian Williams. 2016. “Action, Inaction, Trust, and Cybersecurity’s Common Property Problem.” *IEEE Security & Privacy* 14 (1): 82-86.

Feldman, R., B. Dowd, S. Leitz, and L. A. Blewett. 1997. “The Effect of Premiums on a Small Firm’s Decision to Offer Health Insurance.” *The Journal of Human Resources* 32 (4): 635-658.

FERMA. 2018. Preparing for Cyber Insurance. Brussels: Federation of European Risk Management Associations. https://www.ferma.eu/app/uploads/2019/02/preparing-for-cyber-insurance-web-04-10-2018.pdf.

Gordon, Lawrence A., and Martin P. Loeb. 2002. “The Economics of Information Security Investment.” *ACM Transactions on Information and System Security* 5 (4): 438-457.

Gordon, Lawrence A., Martin P. Loeb, and William Lucyshyn. 2003. “Sharing Information on Computer System Security: An Economic Analysis.” *Journal of Accounting and Public Policy* 22: 461-485.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Tashfeen Sohail. 2006. “The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities.” *Journal of Accounting and Public Policy* 25: 503-530.

Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail. 2003. “A Framework for Using Insurance for Cyber-Risk Management.” *Communications of ACM* 46 (3): 81-85.

Gould, John P. 1969. “The Expected Utility Hypothesis and the Selection of Optimal Deductibles for a Given Insurance Policy.” *The Journal of Business* 42 (2): 143-151.

Gramig, B., R. Horan, and C. Walf. 2005. “A Model of Incentive Compatibility under Moral Hazard in Lovestock Disease Outbreak Response.” *American Agricultural Economics Association 2005 Annual Meeting*. Providence, RI.

Grignon, M., J. Hurley, D. Fenny, E. Guidon, and C. Hackkett. 2018. “Moral Hazard in Health Insurance.” *Economia* 8 (3): 367-405.

Heffley, Dennis R., and Thomas J. Miceli. 1998. “The Economics of Incentive-Based Health Care Plans.” *The Journal of Risk and Insurance* 65 (3): 445-465.

Higgins, Kelly Jackson. 2014. “Cyberinsurance Resurges In The Wake Of Mega-Breaches.” 2 10. Accessed 1 10, 2015. http://www.darkreading.com/perimeter/cyberinsurance-resurges-in-the-wake-of-mega-breaches/d/d-id/1316306.

Hofmann, Annette. 2005. Internalizing externalities of loss-prevention through insurance monopoly: An analysis of interdependent consumer risks. *Working Papers on Risk and Insurance*, Hamburg University.

Hui, K. L., P. F. Ke, Y. Yao, and W. T. Yue. 2019. “Liability-Based Contracts in Information Security Outsourcing.” *Information Systems Research* 30 (2): 411-429.

Hui, Kai-Lung, Wendy Hui, and Wei T. Yue. 2013. “Information Security Outsourcing with System Interdependency and Mandatory Security Requirement.” *Journal of Management Information Systems* 29 (3): 117-156.

Hurtaud, Stephane, Thierry Flamand, Laurent De La Vaissiere, and Afaf Hounka. 2015. “Cyber Insurance as One Element of the Cyber Risk Management Strategy.” Inside (7): 92-97. http://www2.deloitte.com/lu/en/pages/risk/articles/cyber-insurance-element-cyber-risk-management-strategy.html.

Kaplan, Stanley, and John Garrick. 1981. “On the Quantitative Definition of Risk.” *Risk Analysis* 1 (1): 11-27.

Kumar, Ram L., Sungjune Park, and Chandrasekar Subramaniam. 2008. “Understanding the Value of Countermeasure Portfolios in Information Systems Security.” *Journal of Management Information Systems* 25 (2): 241-279.

Kunreuther, Howard, and Geoffrey Heal. 2003. “Interdependent Security.” *The Journal of Risk and Uncertainty* 26 (2/3): 231-249.

Lee, Chul Ho, Xianjun Geng, and Srinivasan Raghunathan. 2013. “Contracting Information Security in the Presence of Double Moral Hazard.” *Information Systems Research* 24 (2): 295-311.

Loch, Karen D., Houston H. Carr, and Merrill E. Warkentin. 1992. “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding.” *MIS Quarterly* 16 (2): 173-186.

Marotta, Angelica, Fabio Martinelli, Stefano Nanni, Albina Orlando, and Artsiom Yautsiukhin. 2017. “Cyber-Insurance Survey.” *Compuer Science Review* 24 (C): 35-61.

Merrey, Paul, Matthew Smith, Matthew Martindale, and Arthurs Kokins. 2017. “Seizing the Cyber Insurance Opportunity: Rethinking Insurers’ Strategies and Structures in the Digital Age.” KPMG International. https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/07/cyber-insurance-report.pdf.

Mitra, Sabyasachi, and Sam Ransbotham. 2015. “Information Disclosure and the Diffusion of Information Security Attacks.” *Information Systems Research* 26 (3): 563-584.

Mookerjee, Vijay, Radha Mookerjee, Alain Bensoussan, and Wei T. Yue. 2011. "When Hackers Talk: Managing Information Security under Variable Attack Rates and Knowledge Dissemination." *Information Systems Research* 22 (3): 606-623.

Noel, Bob. 2017. "Cybersecurity: Shifting the Paradigm from Prevention to Incident Response." ITProPortal.com, 11 August. Accessed September 27, 2019. https://www.itproportal.com/features/cybersecurity-shifting-the-paradigm-from-prevention-to-incident-response/.

OECD. 2017. Enhancing the Role of Insurance in Cyber Risk Management. Paris: OECD Publishing. http://dx.doi.org/10.1787/9789264282148-en.

Ogut, Hulisi, Srinivasan Raghunathan, and Nirup Menon. 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.

Otto, Greg. 2019. "What Capital One's Cybersecurity Team Did (and Did Not) Get Right." 2 August. https://www.cyberscoop.com/capital-one-cybersecurity-data-breach-what-went-wrong/.

Pal, Ranjan, Leana Golubchik, Konstantinos Psounis, and Pan Hui. 2014. "Will Cyber-Insurance Improve Network Security? A Market Analysis." Toronto: *Annual IEEE International Conference on Computer Communications.*

Pashigian, B. Peter, Lawrence L. Schkade, and George H. Menefee. 1966. "The Selection of an Optimal Deductible for a Given Insurance Policy." *The Journal of Business* 39 (1): 35-44.

Pauly, M. V. 1968. "The Economics of Moral Hazard: Comment." *American Economic Review* 58 (3): 531-537.

Perlroth, Nicole, and Elizabeth A. Harris. 2014. "Cyberattack Insurance Can Leave a Lot Uncovered." 9 6. http://www.bostonglobe.com/business/2014/06/08/insurance-protection-for-attacks-computer-systems-challenge/q7vHaHFGujIzZHnrW5DKsO/story.html.

Phelps, Charles E., and Joseph P. Newhouse. 1974. "Coinsurance, the Price of Time, and the Demand for Medical Services." *The Review of Economics and Statistics* 56 (3): 334-342.

PwC. 2014. "Cybersecurity Challenges in an Interconnected World: Key Findings from The Global State of Information Security Survey 2015." pwc.com.

Romanosky, Sasha, Lillian Ablon, Andreas Kuehn, and Therese Jones. 2019. "Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk." *Journal of Cybersecurity* 5 (1): 1-19.

Rowell, D., and L. B. Connelly. 2012. "A History of the Term 'Moral Hazard'." *The Journal of Risk and Insurance* 79 (4): 1051-1075.

Soors, W., N. Devadasan, V. Durairaj, and B. Criel. 2010. *Community health insurance and universal coverage: Multiple paths, many rivers to cross*. World Health Organization.

Stark, John Reed, and David R. Fontaine. 2015. “Ten Cybersecurity Concerns for Every Board of Directors.” CyberSecurityDocker.com. 30 April. http://www.cybersecuritydocket.com/2015/04/30/ten-cybersecurity-concerns-for-every-board-of-directors/#_ftnref12.

Surane, Jenny, and Lananh Nguyen. 2019. “Capital One Breach Clouds Technology Strategy; Puts $400M Cyber Insurance in Play.” 1 August. https://www.insurancejournal.com/news/national/2019/08/01/534388.htm.

Temin, Davia. 2013. “Target’s Worst PR Nightmare: 7 Lessons From Target’s Well-Meant But Flawed Crisis Response.” 30 December. https://www.forbes.com/sites/daviatemin/2013/12/30/targets-worst-pr-nightmare-7-lessons-from-targets-well-meant-but-flawed-crisis-response/#19bca19543cf.

Tham, Irene, and Hariz Baharudin. 2018. “Tardy Responses, Security Failings Led to SingHealth Breach.” 22 September. https://www.straitstimes.com/singapore/tardy-responses-security-failings-led-to-singhealth-breach.

van der Wees, Phillp. J., Joost. J. G. Wammes, Gert. P. Westert, and Patrick. P. T. Jeurissen. 2016. “The Relationship Between the Scope of Essential Health Benefits and Statutory Financing: An International Comparison Across Eight European Countries.” *International Journal of Health Policy and Management* 5 (1): 13-22.

Wang, Jingguo, Aby Chaudhury, and H. Raghav Rao. 2008. “Research Note - A Value-at-Risk Approach to Information Security Investment.” *Information Systems Research* 19 (1): 106-120.

Wang, Tawei, Karthik N. Kannan, and Jackie Rees Ulmer. 2013. “The Association Between the Disclosure and the Realizatio of Information Security Risk Factors.” *Information Systems Research* 24 (2): 201-218.

Whitman, Michael E., and Herbert J. Mattord. 2012. Principles of Information Security. 4th. Boston, MA: Course Technology Cengage Learning.

Yue, Wei T., and Metin Cakanyildirim. 2007. “Intrusion Prevention in Information Systems: Reactive and Proactive Responses.” *Journal of Management Information Systems* 24 (1): 329-353.

Zhao, Xia, Ling Xue, and Andrew B. Whinston. 2013. “Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements.” *Journal of Management Information System*s 30 (1): 123-152.

Zoidze, A., N. Rukhazde, K. Chkhatarashvili, and G. Gotsadze. 2013. “Promoting Universal Financial Protection: Health Insurance for the Poor in Georgia - A Case Study.” Health Research Policy and Systems 11 (45). https://health-policy-systems.biomedcentral.com/articles/10.1186/1478-4505-11-45.

Zweifel, P., and W. G. Manning. 2000. Moral Hazard and Consumer Incentives in Health Care. Vol. 1, Chap. 8 in *Handbook of health economics*, by A. Culyer and J. P. Newhouse, 409-446. Amsterdam: Elsevier.