Inf Syst Front (2019) 21:301–325
DOI 10.1007/s10796-017-9737-3

# A model to analyze the challenge of using cyber insurance

**Tridib Bandyopadhyay**[1] · **Vijay Mookerjee**[2]

Published online: 18 March 2017


**Abstract** This work analyzes and extends insurance dynamics in the context of cyber risk. Cyber insurance contracts, when used as a means to manage residual cyber risk, could behave differently from other traditional (e.g., property) insurance. One important difference arises from the complexity involved in the post-breach decision of whether and how a firm should optimally plan to claim indemnity in the event of a cyber breach. We define different types of cyber breaches leading to different claiming scenarios, whose roots lie in the impact of secondary loss caused by certain but not all types of breaches. We build a model to capture the impact of secondary loss in structuring the use of cyber insurance and then combine the backward analysis of myriad breach scenarios to derive the overall optimal decision to purchase cyber insurance. We demonstrate that the optimal purchase decision depends on the mix of the types of cyber breaches that a firm faces. Numerical experiments corroborate market observation of limited use of cyber insurance after 20 years from when these products became available.

**Keywords** Cyber insurance · IT security management · Cyber risk transfer

## 1 Introduction

As hackers continue to find new ways to circumvent technological controls, it is apparent that security technologies alone do not offer complete immunity from cyber risk (KPMG Inc., 2014). Firms thus use a two-pronged approach to manage IT security risk: first invest in security technologies, and then buy cyber insurance to cover the *residual* IT security risk (Meland et al. 2015). Cyber insurance refers to contracts that stand to mitigate liability issues, property loss, and theft from a data breach. These contracts also cover financial loss from data damage, loss of income from network security failures, cyber-extortion, cyber-terrorism, post incident public relations fees, and criminal reward fund reimbursements (CIO Magazine 2003). Cyber insurance products in the market tend to provide 3 fundamental types of coverage, (a) loss and liability arising out of theft of data, (b) forensic identification and remediation costs to respond to the breach and (c) coverage for legal and regulatory fines and penalties (The Betterly report 2008). In recent times, privacy issues are also being covered in cyber insurance contracts (Floresca 2014).

The size of the US cyber insurance market was originally expected to grow fast and reach $ 2.5 billion in 2005. The market however took a decade longer to reach that level of premium volume ($ 2.5 billion in 2015) and remained very small compared to other insurance markets notwithstanding the fact that cyber insurance has been available in the market for the last 20 or so years (The Betterly Report 2015). For example, a survey across a pool of companies show that on average - for similar levels of exposure between PP&E (property, plant, and equipment) and IA (information assets) risks – the first category was protected with insurance contracts up to 51% of total exposure in the category, whereas the information assets had cyber insurance coverage for only 12% of total exposure in the category (Ponemon LLC 2015). Clearly, cyber

✉ Tridib Bandyopadhyay
tbandyopa@kennesaw.edu

[1] Kennesaw State University, Kennesaw, GA 30144, USA

[2] University of Texas at Dallas, Richardson, TX 75080, USA

insurance products are yet to take a prominent role in managing IT security risks of organizations.

Several reasons have been ascribed for underperformance of cyber insurance, of which industry inexperience; scant empirical data and contract history; and the difficulties in estimating cyber losses (Kovacs et al. 2004) are important. The existence of an apparent monoculture in computing technologies has also been cited for the un-insurability of IT security risk (Bohme 2005). Cyber insurance contracts have also been typically expensive (Nelson and Simek 2005) with no standard pricing models - providers have differed by over 400% in pricing products for the same client (Wood 2007).[1] Finally, recent studies suggest that many companies invest in cyber security as a technology initiative rather than holistically analyzing the cyber risks and treating these investments as strategic initiatives – thereby underappreciating the need and use of cyber insurance instruments (Calandro et al. 2014). In this research, we create a model, analyze in detail and extend the nuances of diffident cyber insurance utilization in the consumption end (Bandyopadhyay et al. 2009).

Consider the following to appreciate the nuanced nature of IT security risk realization and certain counterintuitive observations:

Disclosing a breach incident can adversely impact a firm in multiple ways. Breaches are found to negatively affect stock prices and market capitalization of a firm (Campbell et al. 2003; Cavusoglu et al. 2004). It has also been observed that data breaches can cause abnormal turnover of customers (churn) that may constitute up to 52% of the total cost of a data breach (Ponemon LLC 2008). The top two managerial concerns associated with information security incidents are damage to reputation and brand, and loss of stakeholder confidence (Ernst and Young Inc. 2008). US companies in general suffer from overall reputational and goodwill losses from cyber breaches (Hartwig and Wilkinson 2014). It appears baffling to note that despite the actual reputational losses, cyber insurance products do not pay for lost intellectual property, or the restoration of public confidence and reputation (Steele 2007).

While companies are required to publically disclose breaches involving personally identifiable information loss,[2] other breach incidents often go unreported. Firms fear that consumer confidence will deteriorate with the occurrence of cyberattacks (Kovacs et al. 2004). IT managers cite the fear of 'negative publicity' as one of the top 3 reasons for not reporting realized breaches. The 2002 CSI/FBI survey identifies that about 90% of respondents detected computer security breaches in the past year, yet only 34% reported the attacks to authorities (USA Today, April 2002). Similar observations continue in recent reports (Hartwig and Wilkinson 2014).

Cyber insurance potentially suffers from an under-filing (not filing claims for all cyber coverages) phenomenon. The Ernst and Young Global Information Security Survey (2003) notes that a section of IT managers fear that filing an insurance claim could expose security and intelligence information (Information Security Magazine, August 2004).[3] The numerous information streams in the investigation of a cyber breach by an insurer appointed consultant enhances the likelihood that a breach will get disclosed (Bandyopadhyay et al. 2009). Research also suggests that 'clients fear of damaging publicity if their IT vulnerabilities are revealed make them loathe to file claims' (Baer 2004). In addition, court cases and reports of arbitration settlements suggest that firms find it difficult to show that a breach exposure indeed constitutes 'publication' of stored information, thereby lowering a firm's motivation to file and receive payment for third party liability related claims (McLeod 2015).

The above discussion suggests that managers may decide against filing a cyber insurance claim when they feel that the revealed breach information could damage the reputation of the firm and erode stakeholder confidence or when a claim may be contested in the court because that would make the breach information public. In other words, cyber insurance claim decision could be complicated and may require calculation of the indemnity receivable of a claim *net* of secondary loss (e.g. customer churn, or stock market loss). This possible under-claiming behavior in the context of cyber insurance gives rise to a fundamental demand side problem that resembles *hidden action* problems of information asymmetry (Moore 2005). Further, the presence of secondary loss also creates an interesting pricing problem for the insurance provider: should the provider price the contract to account for such possible under-claiming behavior lest the expected indemnity calculated by the contracting parties differ, thereby making the offered premium structure appear anomalous?

In this work we comprehensively characterize the IT risks arising from a breach, propose a model that captures the nuances of cyber insurance contract in the way it is utilized at an organizational level, analyze the optimal purchase of an cyber insurance contract, derive the price for a cyber insurance product offered by the insurer, investigate the efficiency of the product in managing residual IT security risk at the organizational level and run experiments to provide sensitivities of

[1] For some recent cyber insurance contract pricings (albeit without the deductibles, which are equally determining of the premium structure), please see the pertinent webpage of Data Breach Insurance Inc., USA (https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/)

[2] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#1

[3] It is an understandable posture of the managers. For example, in the 2014 third quarter filing, Home Depot has shown a $15 million cyber insurance receivable (McLeod 2015), which obviously depicts that a severe breach was realized. Had the case been a non-required disclosure breach, the balance sheet or flow statement would have made it apparent to the stakeholders of the event of a breach.

firm parameters in efficient use of cyber insurance instruments and optimal transfer of residual cyber risk to the market.

While the overall contribution of this work is to extend our understanding of traditional insurance to IT risk management and provide directions that may help understand the evolving use of cyber insurance products, the salient insights and contribution of this study are numerous.

We exhibit that ex-post purchase, an insured firm may selectively abstain from claim disclosure for certain types of breaches. We identify, analyze and signify these specific cases. Since the off-contract hidden behavior of the insured firm cannot be credibly signaled, and the pricing of a cyber insurance contract may or may not include the impact of hidden actions in the consumption end, we exhaustively derive both types of optimal contracts and compare them on multiple attributes of success and use of cyber insurance in managing cyber risk. We show that a cyber insurance contract optimally transfers higher amount residual risk when the insurer chooses to consider the off-contract behavior of the insured firm. When this happens, the cyber insurance products are priced attractively. We calculate and provide closed form solutions for specific cases and provide experimental results for the generalized model in regard to optimal levels of pricing and use of cyber insurance contracts. We also check sensitivities of key firm parameters as they impact insurance uptake. Finally, we show that technology firms that are more likely to utilize cyber insurance in their IT risk management programs, face relatively higher pricing in cyber insurance.

The rest of the paper is organized as follows. In Section 2, we review research in IT security and insurance economics. In Section 3, we set up the basic model after providing the background and assumptions. Section 4 analyzes a set of 3 simplified cases under alternate pricing structures for cyber insurance and provides closed form solutions. We conduct numerical experiments with the full-blown model and report the results in section 5. Section 6 discusses these results, provides managerial implications as well as directions for future research. Section 7 concludes the work.

## 2 Related work

Our research brings together issues concerning purchase of cyber insurance to manage the IT security program of an organization. Thus we briefly review the literature in two main areas: (Anderson and Moore 2007) Insurance Economics, (Arrow 1971) Cyber insurance in IT security.

### 2.1 Insurance economics

Mossin and Smith (Mossin and Smith 1968) analyze the rational purchase of insurance by an individual who faces the risk of loss of her wealth, and exhibits a defined preference structure. In their work, an insurance contract is exogenously determined and a balance is sought between the incremental levels of premium and coverage, where the insured chooses the level of deductible or the cap of the contract, and shares a chosen part of her risk with the insurer. On the other hand, using the endogenous framework of Borch (1960) of optimal insurance, Arrow (1971) derives Pareto optimal insurance policies for risk-averse insurers (where coinsurance is optimal) and risk neutral insurers (where full coverage over a deductible is optimal).[4] Schlesinger (1981) investigates optimal levels of deductibles in insurance contracts and shows that conditions like higher loss probability, higher degree of risk aversion, and lower level of initial wealth ensure lower deductibles (more insurance). Like Arrows, this research assumes the insurer (insured) risk neutral (risk averse) such that the offered cyber insurance is Pareto optimal above a deductible. However, in contrast to Schlesinger (1981), the changes in optimal deductible in this research stems from the off-contract behavior of the IT managers.

Gollier (1996) investigates optimal insurance contracts when some risks affecting wealth remains uninsured, and then shows how presence of an uninsurable background risk reduces the policy deductible when the insured behaves in an economically prudent fashion. In another study Gollier and Pratt (1996) explain that an unfair risk affects the willingness of the insuring parties to bear the risks of the existing assets – and conclude that all standard and proper utility functions are vulnerable to risk. In contrast to Gollier's work, our uninsurable (secondary) risks are concomitant but subsequent in nature, and could get triggered when a claim disclosure is made – thereby making the disclosing and claiming of realized loss a strategic decision.

### 2.2 Cyber insurance in cyber security

Gordon et al. (2003) propose a framework of using cyber insurance in mitigating information risk that may not be addressed through technology. They suggest that IT security is a moving target which leaves technology gaps in protection, and that insurance contracts should be in place to repair losses from realized breaches that exceeds organizational risk tolerance. In a contemporary article, Siegel et al. (2002) suggest that technology and process controls must be supported by an insurance framework for successful management of internet security. In this research, the paradigm of a comprehensive framework of cyber risk management is the backdrop while we focus our investigation in the premise of the residual

[4] Raviv extends Arrow"s work and shows that risk preferences do not necessarily determine the forms of an optimal insurance contract and that an optimal contract may feature both deductible and coinsurance. In this research we restrict ourselves with a simple, general deductible based cyber insurance contract

risk of cyber security that remains unmitigated even after the technology controls are implemented.

Nuanced impact of cyber security breach has been explored by scholarly research and discussed in trade press. Information security has been argued to contribute to operational risk incurred by an organization (Fang et al. 2014). Cavusoglu et al. (2004) investigate the observed effects of breach exposure on stock prices of affected firms through an event study, concluding negative impact under general considerations. Campbell et al. (2003) argue that the economic consequences of a reported breach depend on the underlying assets affected by the breach: clarifying that security breaches that involve unauthorized access of confidential data bring higher negative economic impact than otherwise. Johnson (2014) provides one recent compilation of industry surveys and discuss observed impacts of cyber-attacks on firms in terms of categories of losses. Our research recognizes these adverse, disparate exposures from a breach incident, and captures them in the modeling framework to integrate their overall impact on the use of cyber insurance.

Researchers have looked into the scant use of cyber insurance contracts by organizations. Majuca et al. (2006) study the evolution of the market for cyber insurance and explain the effects of traditional impediments like moral hazard and adverse selection for a slow growth of cyber insurance. Bohme and Kataria (2006) study the effect of correlation in cyber risk on the market of cyber insurance. In their work, correlated cyber risk (e.g., virus and worm propagation) is realized at two levels – across multiple systems in a given organization and across similar systems in multiple organizations. Using these two scenarios, their work explains the nuances of demand and pricing of cyber insurance contracts, which together explain the slow growth and size of the cyber insurance market. Bandyopadhyay et al. (2009) provide a framework of asymmetric valuation of cyber insurance contract where the insured firm ends up with a lower indemnity payouts, thereby explaining the firm's reduced interest in cyber insurance. Schwartz et al. (2010) model asymmetry in cyber insurance where ex-post contract behavior of a few rogue users of cyber insurance makes it suboptimal for the insurer to monitor the IT security health of their clientele, thereby negatively affecting the use of cyber insurance. Unlike Bohme and Kataria (2006), this work integrates impact of breaches across all types of losses (not across systems in the same firm or in similar systems across multiple firms) and extends Bandyopadhyay et al. (2009) to explain the challenges that plague the use of cyber insurance.

This research builds on and extends two previous works. First, in the IT risk management area it expands the intuitions from Bandyopadhyay et al. (2009) by creating an analytical model, providing full analysis of the model, and then extending the insights with experimental results on the optimal use of cyber insurance contracts. Second, in the insurance economics area, this work extends Gollier (1996) by internalizing uninsurable background cyber risk which is selectively triggered by the explicit or implicit disclosure of a cyber breach. Unlike other works (Campbell et al. 2003, Cavusoglu et al. 2004 etc.), which narrowly focus only on the impact of cyber breach on stock values of an organization, this study considers all losses from a cyber breach in an inclusive but expansive manner to derive downstream managerial decisions. Further, the insights from this work related to diminished interests in cyber insurance neither stems from correlation of cyber risks across firms (Bohme and Kataria 2006), nor do they result because of the interdependent risks shared between the providers and users of IT risk technology controls (Ogut et al. 2005). Instead, our insights arise from the off-contract rational behavior of firms as they implement cyber insurance contracts.

## 3 The model

We begin with some preliminaries and background of the model together with the notation (Table 1) and assumptions. Next, we derive the claiming strategy of an insured firm when a cyber insurance contract is in place. Finally we derive the insurer"s optimal pricing strategy.

Below we present the types of breach (Bandyopadhyay et al. 2009) and expand on the nature and losses inflicted by them in order to arrive at a set of model parameters.

### 3.1 Breaches

**Symptomatic breach** A symptomatic breach results from an exploitation of firm-specific vulnerabilities, for example, hackers accessing TJMax database for credit card information is an exploitation of the vulnerabilities in the firm-specific data storage arrangement of TJMax. A symptomatic breach provides a negative signal of the efficacy of the IT security program of the firm. Privacy experts believe that the TJMax breach was actually foreseeable (Evers 2007). Symptomatic breaches could also involve failure of capability or trust (e.g., insider attacks) within the firm. Observing a symptomatic breach, stakeholders may downgrade their perception of the IT security health of the firm (The Ernst and Young Survey, 2008), and the firm may suffer additional losses. Not all symptomatic breaches, however, are as well-publicized or cause an impact as large as the TJMax breach. As such, not all but only personally identifiable information breach is required to be publically disclosed (please see footnote 1). Breaches that are of lesser magnitude could escape the public eye. A firm, afflicted by a symptomatic breach, has the motivation not to disclose the breach information to its stakeholders within the bounds of accounting norms, compliance requirements and regulatory obligations.

**Table 1** Notation for model parameters and decision variables

| | |
|---|---|
| $F_i$ | Insuring firm, offering cyber insurance (assumed risk neutral) |
| $F_d$ | Insured firm, buying cyber insurance (assumed risk averse) |
| $W$ | Insured firms beginning wealth, a constant |
| $q$ | Probability of an IT security breach |
| $\delta$ | Conditional probability of a symptomatic breach: P(symptomatic breach \| breach) |
| $\gamma$ | Conditional probability of a private breach: P(private breach \| symptomatic breach) |
| $x$ | Insured firms realization of primary (cyber) loss, given a breach |
| $f(x)$ | Distribution of the Insured firms primary cyber loss (assumed common knowledge between the contacting parties), given a breach |
| $P$ | Upfront premium for the cyber insurance contract |
| $\Gamma$ | Insured firm"s claim strategy for a private breach |
| $I$ | Indemnity payout, $I(x) \geq 0$, $I'(x) \geq 0$, |
| $G$ | Secondary loss subsequent to a certain type of realized breach |
| $U$ | Insured firms utility function (assumed concave) |
| $\lambda$ | Insured firms proportional risk loading factor – a standard industry norm |

**Systemic breach** Arising fundamentally out of the usage of basic IT systems and interconnectivity in business processes, a systemic breach occurs when the affected firm has no reasonable or known way to defend against the breach, especially when the attack is transmitted through business networks (e.g., MyDoom virus infected 8% of e-mail traffic in US and took down numerous mail servers). Such breaches could also be the effects of a zero-day vector designed to affect a popular operating environment or software (e.g., Microsoft Internet Information Services Remote Buffer Overflow). The differentiating characteristics of systemic breaches are that (a) there is no firm-specific malice intended, and that (b) no firm-specific or IT security program-specific vulnerabilities are exploited. Stakeholders are therefore unlikely to revise their perception of the security health of the firm for a realized systemic breach because (a) IT security programs can only plan for known threats, and (b) firms must operate in the networked economy and accept systemic cyber risks as the cost of doing business. These breaches are likely to be considered as standard risks of employing IT assets and doing business in networked world (Computer weekly, 2000) or cost of doing business (ISSA, 2008).[5] As a result, an affected firm has no motivation and sometimes no ability either to conceal a realized systemic breach.

**Public breach** A breach is public if it satisfies one or more of the following. First, the breach is publicly observable, e.g., a DDoS attack that impairs transactions. For example, Mininova Inc., one of the leading BitTorrent sites, suffered from a massive DDoS attack over a period of several days in March, 2009 (TorrentFreak, 2009). Second, the breach must be disclosed for legal reasons. For example, State of California"s seminal data breach disclosure law *SB 1386*, now ratified by 38 more states (Berinato 2008). Finally, the breach requires disclosure by an accounting rule or norm deemed necessary by professional practices, e.g., *materiality* of accounting loss, FASB/GAAP definitions and auditing standards, e.g., SAS-107, 2006.

**Private breach** Breaches, that are not public, are private by this definition.

### 3.2 Losses

**Primary loss** Primary (or cyber) loss includes loss of data, information and network assets, etc., and the associated costs. These losses manifest in business discontinuity or disablement, and could include property, rights or transactional losses; maintenance and recovery expenses; contractual losses and liabilities. Direct costs could include core process related activities that drive expenditures for (a) *detection*: discovery of the breach, e.g. manual inspection of IDS alarms, (b) *escalation*: in-firm containment activities, e.g., triggering the incidence response and disaster recovery plans into effect, (c) *notification*: intimation to the data subjects (e.g., email, fax, letter, etc., to the affected parties) and (d) *ex-post response*: activities and recommendations to minimize losses, e.g. offering credit monitoring facility to customers whose personal information was lost (Ponemon Study 2008). Not all breaches cause all these expenditures. Loss of business or loss of proprietary content may not require any response outside organization but the loss of asset is realized. The primary loss appears as an uncontrollable first degree effect in all of the above breach scenarios, i.e., under all combinations of public or private and systemic or symptomatic breaches. All first and third party losses that are directly attributable to the breach incident are primary losses, and may be covered in the cyber insurance contract.

[5] The Great Debate, ISSA journal 2008, available at http://cdn.coverstand.com/1336/3515/ISSA_0408_bt.pdf

**Secondary loss** Secondary losses stem from the loss in stakeholder confidence when information about a breach incident reaches them. We differentiate between primary and secondary loss in the following fashion: secondary loss is an indirect effect that is triggered by the perception of lowered security health of the breached firm when breach information is disclosed. Secondary losses have been noted under various names and suggestions: (a) *opportunity costs* including turnover of existing customers and diminished acquisition of new customers (Ponemon Study 2008), (b) *damage* to reputation, brand, employee relationship, and stakeholder confidence (E&Y Survey. 2008), (c) *market loss* (Cavusoglu et al. 2004) and (d) *damaging publicity* (Baer 2004). Importantly, secondary loss occurs only under certain scenarios (Fig. 1).

The secondary losses may continue to occur much after a breach incident, and these losses are not covered in a contract written for cyber loss - cyber insurance does not pay for lost intellectual property, cost of restoring public confidence or damage to reputation (Steele 2007, Hartwig and Wilkinson 2014). Secondary losses could greatly vary in magnitude; some analysis suggests that the losses associated with customer churn and diminished acquisition could be as high as 52% of the total cost (Ponemon Study, 2008).

Figure 1 depicts the relationship between the types of cyber breach and the loss that the firm incurs from these breaches. Both public and private breaches bring primary losses. However, primary loss is also followed by secondary loss when the breach is symptomatic and the breach information reaches the stakeholders in an explicit or implicit fashion. Although studies have empirically established the existence of secondary losses for information compromises (Campbell et al. 2003; Cavusoglu et al. 2004), and industry research notes that the IT managers expect and acknowledge these losses (The EY Survey 2008, Richardson 2008, The Ponemon Study 2008), the nature and magnitude of these losses are not fully known yet. Further, only certain types of breaches, when disclosed, adversely impact stock prices (Campbell et al. 2003). On the other hand, realization of secondary loss can be controlled by the victim firm under certain considerations (e.g., withholding the disclosure of the breach event and/or refraining from claiming the losses) – a more detailed understanding of which has been provided in subsection 3.6 where we describe the insurance contract timeline.

### 3.3 Notation and assumptions of the study

#### *3.3.1 Assumptions*

We make the following four assumptions:

1) The loading factor $\lambda$ in the cyber insurance contract is proportional to the expected indemnity payout - a common assumption from the insurance literature (Bowers et al. 1997).
2) The primary (cyber) loss function $f(x)$ is common knowledge between the contracting parties in cyber insurance. The assumption of this transparency simply follows from the actual market practice when a contract is drawn.[6] It also implies competitively priced contracts when $\lambda$is an industry norm – which is often the case. This assumption allows our model to provide insights that remain valid notwithstanding the supply-side frictions (e.g., issues regarding the difficulties in quantifying residual cyber risk or inadequate history of claim data etc.) in the cyber insurance market.
3) Claiming is an ex-post breach (after insurance purchase and breach realization) decision which includes an understanding that the process of claiming may expose breach to investors through various routes of information dissemination and financial statements (Bandyopadhyay et al. 2009).
4) The secondary loss of the insured firm is an arbitrary constant $G$.

### 3.4 The cyber insurance contract

We begin with an established result that a risk-averse firm purchases full insurance coverage above a deductible, when the offered premium structure depends on the contract"s actuarial value (Arrow 1971). A cyber insurance contract is a couple ($P$, $I$), so that when the insured pays an upfront premium $P$, the insurer promises an indemnity payment $I(x)$ in the event of a cyber loss of magnitude $x$. The premium $P$ depends on the probability distribution of cyber losses $x$ $(0 \le x \le \infty)$ of the insured firm and the market-loading factor $\lambda$, which includes third party security readiness assessment fees and contract writing costs. Because we assume that the market-loading factor is proportional to the expected indemnity payout of the insurer, and that the insurer is risk neutral, the insurer offers a Pareto-optimal cyber insurance contract above a deductible $x_1$ (Raviv 1979). Assuming that claims for losses above the deductible are payable in full, the indemnity payout and the upfront premium are given by:

$$\begin{aligned} I(x) &= 0 && 0 \le x \le x_1 \\ I(x) &= x - x_1 && x > x_1 \end{aligned} \tag{1}$$

$$P(x_1) = q.(1+\lambda)\int_{x_1}^{\infty}(x - x_1)f(x)dx \tag{2}$$

[6] In practice, cyber insurance providers employ interviews, questionnaires and other instruments as well as technical audits to appraise themselves of the state of residual risk after the technological controls are in place. The insured firm must agree to these inquisitions before a cyber insurance contract is written by the insurer.

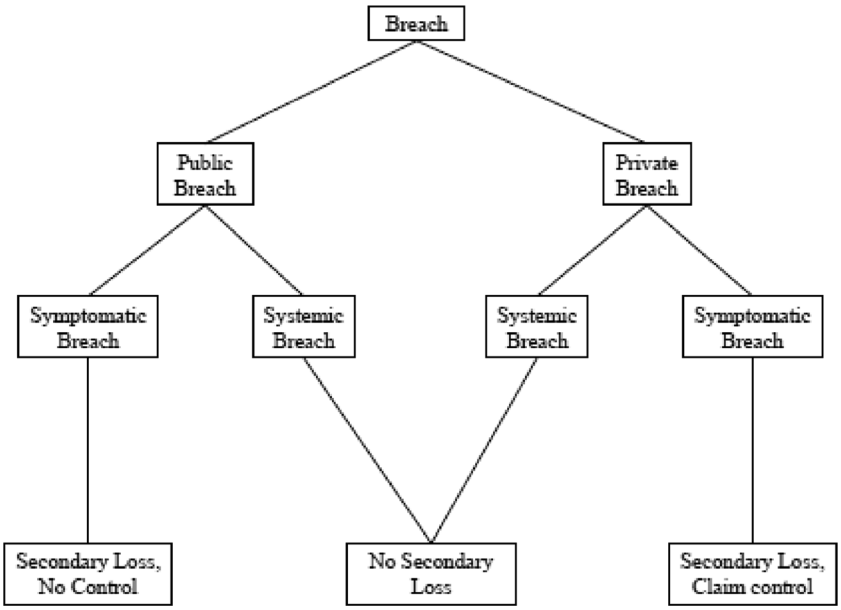



**Fig. 1** Types of realized breach and the loss to the firm

Where $q$ and $f(x)$ are the probability and loss distribution of the breach respectively. The insured firm chooses the deductible $x_1$, which determines the premium $P$.

### 3.5 The contract time line and the payoffs to the parties

We consider a simple form of insurance contract. At the beginning of the period, a contract is written. As per standard market practices,[7] an insured firm undergoes a risk [$f(x)$] evaluation process through questionnaire, interview and other assessment processes before a cyber insurance contract is written. At the end of this process, the firm chooses its optimal deductible $x_1^*$ and the insurer offers a Pareto optimal contract ($P^*$, $I^*$), the form of which is represented by (1) and (2). If the optimal deductible is 0, the insured firm buys full insurance (100% transfer of *residual* IT security risk). In case the optimal deductible is infinitely high, the premium is $P^*=0$, in other words, there is no contract and the insured firm accepts all residual cyber risks (*self- insurance*). Between these two extremes in the deductible, contracts are written to optimally transfer an optimal part of the residual IT security risk to the insurer. The factor $\lambda$ as assumed, is a market rate of loading.

A breach is realized with probability $q$, and the firm incurs the cyber loss $x$. The probability that a breach is symptomatic, is $\delta$. A symptomatic breach becomes public with probability $(1-\gamma)$. The disclosure of a public breach incident is automatic, and the firm incurs the secondary loss $G$. The insured firm then claims for the primary (cyber) loss, and realizes the indemnity payout. On the other hand, a symptomatic breach is of private type with probability $\gamma$ and the secondary loss $G$ is incurred only when the insured firm claims. Else, only the cyber loss$x$is incurred. The above scenarios have been depicted in Fig. 2, together with the utility of the insured firm.

Note that the dominated strategies of a) *no-claim* following (i) symptomatic public breach and (ii) systemic public or private breach, and b) legal impossibilities like *claim when no breach* have been *suppressed* in the diagram. Also, because a systemic breach (by definition) does not bring secondary loss, the private and public systemic breaches have been combined (the claim decisions and hence the expected utilities remain unchanged either way). The payoff to the risk neutral insurer is the upfront premium, which is the indemnity payout, loaded with the factor $\lambda$.

### 3.6 The insured firm"s decision problem

The insured firm chooses its optimal deductible $x_1^*$, and receives a Pareto optimal cyber insurance contract $\left(P^*,\ x_1^*\right)$. For a *public breach*, the insured firm"s dominant strategy is to claim the realized losses. However, for a *private symptomatic breach*, the insured firm implements its optimal claim strategy $\Gamma$. This claim strategy affects the overall optimal deductible $x_1^*$. Thus, we utilize backward induction in the following fashion. First we find the optimal claim strategy for a given deductible, and then calculate the optimal deductible $x_1^*$, which maximizes the expected utility of the insured firm.

Define the claim strategy in private symptomatic breach in the form of an indicator function: $\Gamma(x)=1$ when the insured firm claims a realized cyber loss $x$ from a private symptomatic breach, else $\Gamma(x)=0$. Since we assume a breach (event)

[7] For example see www.aig.com, www.chubb.com etc. by visiting their cyber insurance product pages

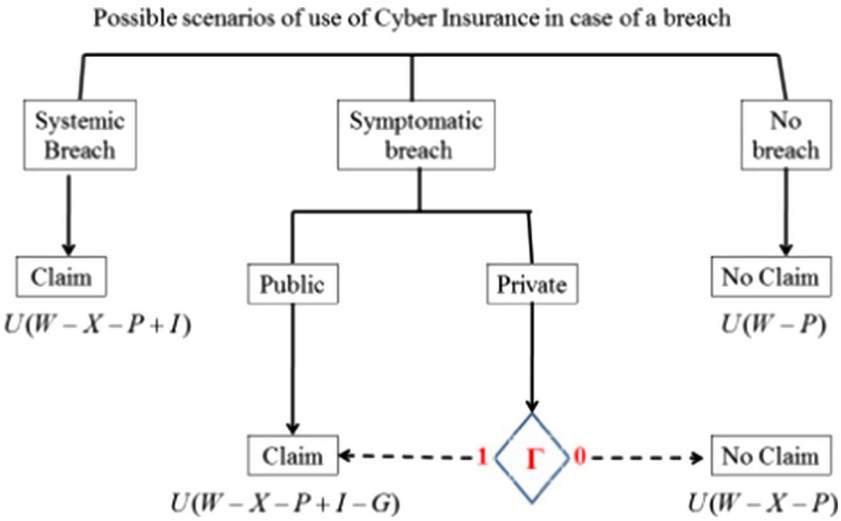



**Fig. 2** The simplified tree for decisions and resultant utility of the insured firm

oriented secondary loss $G$, $\Gamma(x)=1$ implies only a full claim decision. The processes and information channels associated with claiming brings the secondary loss $G$. In other words, it is a *dominant strategy* to claim all losses once it is optimal to claim losses from a private symptomatic breach (Fig. 3, and proposition-1). Claiming more than the realized loss is illegal by contract design. Given the claim strategy $\Gamma(x)$, the insured firm maximizes (Bandyopadhyay et al. 2009) to arrive at its optimal deductible $x_1^*$ .

The first term in (Bandyopadhyay et al. 2009) refers to a *private symptomatic* breach (probability, $q\delta\gamma$). Claiming a private symptomatic breach means tacit exposure of the breach, but the firm is able to weigh the costs and benefits of the claiming decision under an indemnity payment of $I=\Gamma(x)I(x)$. Note that the secondary loss in the private breach is incurred when a claim is made (i.e., if $\Gamma(x)=1$). The second term represents a *public symptomatic* breach (probability $q\delta(1-\gamma)$), where the secondary loss is anyway incurred, and the managers do claim indemnity for the loss. The third term refers to a *systemic* breach (probability: $q(1-\delta)$ ). Here, the firm suffers primary cyber loss$x$, but there are no secondary losses to consider. Thus the firm claims the cyber loss and realizes the indemnity payout. The fourth term refers to a no-breach situation (probability $1-q$).

$$
\begin{aligned}
&q\delta\left\{\gamma\int_0^{\overline{g}}\int_0^{\infty}U(W-x-P+\Gamma(x)I(x)-\Gamma(x)G)\,f(x)h(G)\mathrm{dxdG}\right.\\
&\left.+(1-\gamma)\int_0^{\overline{g}}\int_0^{\infty}U(W-x-P+I(x)-G)\,f(x)h(g)\mathrm{dxdG}\right\}\\
&+q(1-\delta)\int_0^{\infty}U(W-P-x+I(x))\,f(x)dx\\
&+(1-q)\int_0^{\infty}U(W-P)\,f(x)dx
\end{aligned}
\tag{3}
$$

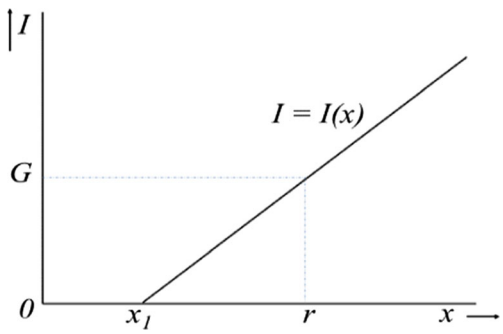



**Fig. 3** The deductible ($r$) in a private symptomatic breach, and the contracted deductible $x_1$

**Proposition 1** *For a secondary lossGassociated with a realized private symptomatic breach event, there exists a minimum loss r* $(=x_1+G)$ *up to which the insured firm does not claim. For losses above r, the insured firm claims its actual loss.*

The formal proof is provided in Appendix Section 1. Informally, first note that the claim decision variable only appears in the first term of the above objective function. Then use the fact that the functional $\Gamma(x)(I(x)-G)$ is linear in $\Gamma$. Hence we get a *bang-bang* solution; i.e.,$\Gamma(x)=0$, if $I(x)-G<0$ ; $\Gamma(x)=1$, otherwise. The proof follows.

Note that in the case of private symptomatic breaches, the existence of secondary loss increases the effective deductible of the cyber insurance contract, and contrary to the contracts designed behavior, the insured firm does not claim its losses in the range $x_1\le x\le r$, $(r=x_1+G)$. A cyber insurance contract with a *unique* deductible cannot alter this *no claim* strategy of the insured firm in the range $x_1\le x\le r$ because of the probabilistic realization of private symptomatic breaches. In effect, unclaimed loss in the range $x_1\le x\le r$ exhibits a

reducing effect on the overall expected indemnity from the cyber insurance contract.

As we demonstrate later, such extra contractual behavior impacts the pricing of the contract. The claim decision being ex-post, the insured firm suffers from an inherent inability to credibly signal probabilistic underclaiming for certain types of breaches. This frees the insurer to selectively include/exclude such implicit but probabilistic ex-post claim behavior in pricing the contract.

### 3.7 The optimum deductible for the contract

Incorporating the claiming strategy from Proposition 1 and the associated indemnity payout for a private symptomatic breach, expression (3) modifies to (Baer 2004). The solution of the modified problem yields the optimal deductible $x_1^*$, which is communicated to the insurer. Now we show how the premium $P$ depends on the probabilistic scenario of proposition 1.

$$\underset{x_1}{Max}\begin{pmatrix} q\delta\gamma\left(\int_0^{x_1+G} U(W-x-P(x_1))f(x)dx + U(W-x_1-P(x_1)-G)(1-F(x_1))\right)+ \\ q\delta(1-\gamma)\left(\int_0^{x_1} U(W-x-P(x_1)-G)f(x)dx + U(W-x_1-P(x_1)-G)(1-F(x_1))\right)+ \\ q(1-\delta)\left(\int_0^{x_1} U(W-x-P(x_1))f(x)dx + U(W-x_1-P(x_1))(1-F(x_1))\right) + (1-q)U(W-P(x_1)) \end{pmatrix} \tag{4}$$

### 3.8 The insurer"s pricing decision problem

We consider two pricing strategies: *traditional*, and *adjusted*. In the traditional pricing strategy, the premium is calculated like that in any standard insurance contract without considering the impact of secondary loss on claiming behavior. The adjusted pricing strategy takes into consideration the probabilistic extra-contract behavior. In adjusted pricing, the premium is charged assuming that the insured firm will not claim for a private, symptomatic breach if the loss amount is less than the deductible plus the expected secondary loss. The pricing structures for a cyber insurance contract for a deductible $x_1$ for the pricing structures are provided below.

1) Traditional Pricing

$$P_1(x_1) = q.(1+\lambda)\int_{x_1}^{\infty}(x-x_1)f(x)dx \tag{5}$$

2) Adjusted Pricing

$$P_2(x_1) = q\,\delta(1+\lambda)\left(\gamma\int_{x_1+G}^{\infty}(x-x_1)f(x)dx + (1-\gamma)\int_{x_1}^{\infty}(x-x_1)f(x)dx\right) + q\,(1-\delta)(1+\lambda)\int_{x_1}^{\infty}(x-x_1)f(x)dx \tag{6}$$

**Lemma 1** *For any given deductible, the premium structure under adjusted pricing is never higher than that under traditional pricing* i.e. $P_1(x_1) \geq P_2(x_1)$ .

*Proof* Please see appendix section 1.

Note that the expected utility of the insured firm depends on the structure of the premium (Baer and Parkinson 2007) or (Bowers et al. 1997) to be used in (Baer 2004). Lemma 2 qualifies the extent of overpricing that occurs in the traditional pricing structure.

**Lemma 2** *For a selected deductible* $x_1$ , $x_1 \geq 0$ , *overpricing* $(P_1 - P_2)$ *under traditional pricing and uniformly distributed primary loss in the range [a, b]:*

1) *Increases linearly with the probability of private breach* $\gamma$
2) *Exhibits quadratic increase with the expected secondary loss* $G$

*Proof* Please see appendix section 1.

Lemmas 1 and 2 compare the two pricing structures. The pricing structure, being a funal in (Baer 2004), affects the optimal deductible. In other words, the optimal deductible that the insured firm communicates to the insurer will be dependent on the pricing structure offered by the insurer. The deductible determines the *proportion of IT security risk* that the insured firm would be able to transfer to the insurer. A lower deductible indicates that the contract transfers a higher amount of risk to the insurer. In the next section, we compare the two pricing structures from the perspective of (a) the profit earned by the insurer, and (b) the optimal IT security risk transferred by the cyber insurance contract, i.e., the success of cyber insurance.

## 4 Impact of pricing on insurer profit and transfer of risk

In section 3, we have shown that for the *same* deductible, traditional pricing leads to a higher premium. Our goal in sections 4 and 5 is to calculate and compare the efficiency of the cyber insurance contracts as residual risk transfer

instruments under the two pricing structures. We also compare the value of the contract to the contracting parties under the two kinds of pricing.

The claim decision being ex-post, the insured firm cannot credibly signal probabilistic underclaiming for certain types of breaches, and the insurer chooses whether to include such implicit but probabilistic ex-post claim behavior while pricing the contract structure. Finally, given a pricing structure, the optimal deductibles differ. Thus an interesting question to pose is: given that the premium for the same deductible is always higher for traditional pricing, can the lower, adjusted pricing do better for an insurer? While the short answer to this question is yes, the full-blown analysis of this issue is difficult - as we progressively demonstrate in this section. In order to facilitate understanding, however, we analyze three special cases that accentuate the difference between the payoffs from traditional and adjusted pricings facing specific conditionality. One of the main insights we derive from the analysis in this section is that cyber insurance has the flavor of both traditional insurance and non-traditional insurance. The traditional part corresponds to public, systemic breaches where the insured firm always claims and there is no secondary loss, or where the firm suffers other uncontrollable losses as in the case of a public, symptomatic breach. The non-traditional part corresponds to situations where the firm"s failure to protect its information assets causes a secondary wave of losses - as in the case of a private symptomatic breach. By mixing the flavors of traditional and non-traditional insurance, we get an insurance problem that is quite challenging to analyze.

### 4.1 Three special cases

#### *4.1.1 Case a*

Case A is constructed to be biased in favor of adjusted pricing. Here, we consider a case where secondary losses accompany every claim; that is, all losses are private and symptomatic. The loss function is such that there are two possible losses, $a$ (small loss, with probability$p$) and $b$ (large loss, with probability $1-p$ ). Let the expected secondary loss ($G$) be such the insured firm does not claim for the small loss but always claims when the loss is large. To summarize, the specific conditions imposed on the general model that characterize Case A are:

$$q = \delta = \gamma = 1; U(y) = Ln(y), f(x): \quad a \rightarrow p, b \rightarrow (1-p); a < G < b$$

This simple case can be analyzed to gain insights into the two pricing structures. To facilitate the analysis, we first establish that when the chosen deductible is greater than or equal to $a$ , the two pricing structures will offer the same premium. This is clear because when the deductible is greater than or equal to $a$, even the traditional pricing cannot consider the lower loss ($a$) in the calculation of the premium. Adjusted pricing, of course, would ignore the lower loss, knowing that the insured firm will never claim for the lower loss. Thus the two pricing structures will behave in exactly the same way (and hence, yield the same profits for the insurer) if the deductible is greater than or equal to $a$. We therefore need to focus on the case where the deductible is less than $a$ and compare the insurer's profits to see which contract (traditional or adjusted) does better from the perspective of the insurer.

First, let us consider the traditional pricing. The premium charged and the corresponding utility function for the insured firm with a deductible $x_1$ are given by

$$P_1 = (1+\lambda)(p(a-x_1) + (1-p)(b-x_1))$$
$$U_1 = pLn(W-a-P_1) + (1-p)Ln(W-x_1-P_1-G)$$

If the value of $P_1$ is substituted in the utility function $U_1$ , an optimization of $U_1$ with respect to $x_1$ yields the result that for $0 \le x_1 \le a$ , the optimal value of $x_1$ , $x_1^* = a$ . To establish this, it is easy to show that the derivative of $U_1$ with respect to $x_1$ is positive in the range $0 \le x_1 \le a$ . Hence, we get a boundary solution for the deductible ($a$). We note next that for any deductible$x_1$, traditional pricing earns a profit $P_1 - \frac{P_2(x_1)}{1+\lambda}$, where $P_2(x_1)$ is the premium charged for the same deductible under adjusted pricing. Substituting the value of the optimal deductible ($x_1^* = a$ ) in the profit function, we obtain the profit expression for traditional pricing:

$$\Pi_1 = \lambda(1-p)(b-a) \tag{7}$$

Next we consider the case of adjusted pricing. The premium charged changes to $P_2 = (1+\lambda)(1-p)(b-x_2)$, where $x_2$ is the deductible chosen by the insured firm. As established earlier, we again focus only on the range $0 \le x_2 \le a$ . For any choice of the deductible in this range adjusted pricing will earn a profit given by

$$\Pi_2(x_2) = \lambda(1-p)(b-x_2) \tag{8}$$

If we compare (Mader 2002) and (Bohme 2005), it is clear that adjusted pricing will always earn a higher profit if the deductible is chosen in the range $[0, a)$ . Thus, the conditions prescribed under Model A provide a *one sided* result, namely, that *the insurer is weakly better off under adjusted pricing than traditional pricing.* What, if any, is the motivation for traditional pricing for the insurer? Model B below addresses that question.

*4.1.2 Case B*

To illustrate a two sided result yet maintain analytical tractability, we replace the Constant Relative Risk Aversion (CRRA) utility function $U(y)=Ln(y)$with a Constant Absolute Risk Aversion (CARA) utility function $U(y)=1-e^{-\alpha y}$ where $\alpha$ is a constant. Assume that a breach happens with probability $q$, and that the breach is systemic with probability $p$. For a systemic breach, the loss is $a$, and there is no secondary loss. In the symptomatic case, the breach is assumed private. The expected secondary loss $G$ is so assumed that the insured firm is unable to claim for the private symptomatic breach. The premiums under traditional and adjusted pricing are $P_1=q(1+\lambda)(a-x_1)$ , $P_2=pq(1+\lambda)(a-x_2)$ respectively.

The general expression for the expected utility of the insured firm ($i\in\{1,2\}$) is:

$$U_i = qp\left(1-e^{-\alpha(W-P_i-x_i)}\right)+q(1-p)\left(1-e^{-\alpha(W-P_i-a)}\right)+(1-q)\left(1-e^{-\alpha(W-P_i)}\right)$$

When $P_i$ is suitably substituted, optimizing $U_i$ yields the optimal deductible $x_i^*$ selected by the insured firm:

$$x_1^* = \frac{1}{\alpha}Ln\left(\frac{\phi}{p(1-q(1+\lambda))}\right)$$

$$x_2^* = \frac{1}{\alpha}Ln\left(\frac{\phi}{1-pq(1+\lambda)}\right)$$

Where, $\phi=(1+\lambda)\{q(1-p)e^{\alpha a}+(1-q)\}$ .

Before we compare the profits of the insurer, it is interesting to note that the cyber insurance contract under adjusted pricing transfers a higher amount of residual risk:

$$0\le p\le 1, 0\le q\le 1, \lambda\ge 0 \quad\Rightarrow\quad p(1-q(1+\lambda))\le 1-pq(1+\lambda)\Rightarrow\quad x_2^*\le x_1^*.$$

The expected indemnity payout for the contract is $pq\left(a-x_i^*\right)$, and the profits of the insurer are

$$\Pi_1 = q\left(a-x_1^*\right)(1-p+\lambda)$$

$$\Pi_2 = \lambda pq\left(a-x_2^*\right)$$

For a specific cyber loss $a=a^*$, in order for both pricing structures to yield the same profit:

$$\frac{a^*-x_1^*}{a^*-x_2^*} = \frac{\lambda p}{1-p+\lambda}$$

Clearly, if $a<a^*$ , then adjusted pricing, and if $a>a^*$ then traditional pricing fares better for the insurer.

Although analytical tractability issues prevent close form results for the CRRA (logarithmic) utility function, the above two-sided result is not unique to the CARA function. As shown in the quick example below, the more general logarithmic utility function can also provide a similar result like the CARA function:

**Example**: Fix $W=2000$ , $\alpha=0.003$ , $p=0.8$ , $q=0.2$ , $\lambda=0.3$ .

Under the CARA (exponential) utility function, $a^*=318$ . Check, if $a=300$ , $\pi_1^*=7.35$ and $\pi_2^*=8.18$ and if $a=400$ , $\pi_1^*=16.09$ and $\pi_2^*=12.38$ .

Under the CRRA (logarithmic) utility function[8] $a^*=1273.4$ . If $a=1000$ , $\pi_1^*=3.95$ and $\pi_2^*=19.44$ and if $a=1500$ , $\pi_1^*=47.88$ and $\pi_2^*=36.63$.

As case-B illustrates, the insurer could be better off in either traditional or adjusted pricing. However, the insured firm is never worse off with the adjusted pricing. This is clear because for any deductible, the insured firm receives the same indemnity payout at a smaller premium under adjusted pricing.

Unlike cases A and B, where the loss structures were deterministic and discrete, we now include a more realistic continuous, stochastic loss distribution to the cyber insurance problem and investigate implications of pricing structure on the levels of optimally transferred cyber risk.

*4.1.3 Case C*

Now assume that the cyber loss is distributed as $f(x), 0\le x\le\infty$ , all losses are symptomatic and that public breaches occur with probability$q$. As in case B, we continue with the CARA utility function $U(y)=1-e^{-\alpha y}$ for analytical tractability. The traditional and adjusted premium structures including their FOCs, as well as the expected utility of the insured firm are as follow:

$$P_1(x_1) = (1+\lambda)\int_{x_1}^{\infty}(x-x_1)f(x)dx; \quad \frac{dP_1}{dx_1} = -(1+\lambda)(1-F(x_1))$$

$$P_2(x_2) = (1+\lambda)\left[q\int_{x_2}^{\infty}(x-x_2)f(x)dx + (1-q)\int_{x_2+G}^{\infty}(x-x_2)f(x)dx\right]$$

$$\frac{dP_2}{dx_2} = -(1+\lambda)[q(1-F(x_2)) + (1-q)(1-F(x_2+G)+Gf(x_2+G))]$$

$$U(x_i) = q\left[\int_0^{x_i}\left(1-e^{-\alpha(W-x-P_i-G)}\right)f(x)dx + \int_{x_i}^{\infty}\left(1-e^{-\alpha(W-x_i-P_i-G)}\right)f(x)dx\right]$$

$$+(1-q)\left[\int_0^{x_i+G}\left(1-e^{-\alpha(W-x-P_i)}\right)f(x)dx + \int_{x_i+G}^{\infty}\left(1-e^{-\alpha(W-x_i-P_i-G)}\right)f(x)dx\right]$$

The FOC of the expected utility of the insured firm can be represented as:

$$\frac{dU(x_i)}{dx_i} = -\alpha e^{-\alpha(W-P_i-G)}\left[\varphi_3(x_i)+\frac{dP_i}{dx_i}\varphi_4(x_i)\right], \text{where}$$

$$\varphi_1(x_i) = \int_0^{x_i}e^{\alpha x}f(x)dx; \quad \varphi_2(x_i) = \int_0^{x_i+G}e^{\alpha x}f(x)dx$$

$$\varphi_3(x_i) = e^{\alpha x_i}\left[q\left(1-F(x_i)+(1-q)(1-F(x_i+G)\right)\right]$$

[8] While the other expressions including the premiums and the profit functions remain same as those in CARA, the utility function for the CRRA function is $U=qpLn(W-P-x_1)+q(1-p)Ln(W-P-a)+(1-q)pLn(W-P)$.

$$\varphi_4(x_i) = \varphi_3(x_i) + q\varphi_1(x_i) + (1-q)\varphi_2(x_i)$$

We next evaluate the slope of $U(x_2)$ at $x_1^*$ , the optimal deductible under traditional pricing

$$\left(\frac{dU(x_2)}{dx_2}\right)_{x_2=x_1^*} = -\alpha e^{-\alpha\left(W-P_2\left(x_1^*\right)-G\right)}\left[\varphi_3\left(x_1^*\right) + \varphi_4\left(x_1^*\right)\left(\frac{dP_2}{dx_2}\right)_{x_2=x_1^*}\right]$$

However, by definition of $x_1^*$ , we know that

$$-\alpha e^{-\alpha\left(W-P_1\left(x_1^*\right)-G\right)}\left[\varphi_3\left(x_1^*\right) + \frac{dP_1\left(x_1^*\right)}{dx_1}\varphi_4\left(x_1^*\right)\right] = \left(\frac{dU(x_1)}{dx_1}\right)_{x_1=x_1^*} = 0,$$

Thus indicating

$$\left[\varphi_3\left(x_1^*\right) = -\frac{dP_1\left(x_1^*\right)}{dx_1}\varphi_4\left(x_1^*\right)\right]$$

We can write,

$$\left(\frac{dP_1}{dx_1}\right)_{x_1=x_1^*} = -(1+\lambda)\left[q\left(1-F\left(x_1^*\right)\right) + (1-q)\left(1-F\left(x_1^*\right)\right)\right]$$

We can also evaluate,

$$\left(\frac{dP_2}{dx_2}\right)_{x_2=x_1^*} = -(1+\lambda)\left[q\left(1-F\left(x_1^*\right)\right) + (1-q)\left(1-F\left(x_1^*+G\right) + Gf\left(x_1^*+g\right)\right)\right]$$

Substituting $\varphi_3\left(x_1^*\right)$ , $\left(\frac{dP_1}{dx_1}\right)_{x_1=x_1^*} and \left(\frac{dP_2}{dx_2}\right)_{x_2=x_1^*}$ in $\left(\frac{dU(x_2)}{dx_2}\right)$ $x_2 = x_1^*$

We obtain the required criterion ($\zeta$):

$$\zeta = F\left(x_1^*+G\right) - F\left(x_1^*\right) - Gf\left(x_1^*+G\right)$$

If $\zeta = 0$ , the optimal deductibles under the two pricing schemes are equal. Else, if $\zeta > 0$ , then $x_1^* > x_2^*$ , otherwise, $x_1^* < x_2^*$ .

Several general *insights* emerge in this section. First, there are plausible circumstances in cyber insurance (e.g., the level of cyber loss faced by a firm) when either traditional or adjusted pricing could prove more profitable to the insurer. Second, the insured firm is never worse off under the adjusted pricing. And finally, the actual level or distribution of the loss function faced by the insured firm could influence the relative levels of optimally chosen deductibles and hence the optimal levels of cyber risk transfer under the traditional or adjusted pricing. In order to investigate these circumstances all together in a general setting, we will need to consider all the elements of the problem, rather than the simplified cases considered in this subsection. The analysis of a general setting is analytically intractable. We now resort to numerical analysis to obtain detailed insights. The numerical analysis utilizes a CRRA (logarithmic) utility function.

## 5 Analysis of The full model

We employ $U(.) = Ln\ (.)$ for the utility of the insured firm and uniform loss distribution $f(x) = 1/(b-a)$ , $a \le x \le b$ for the cyber loss covered in the contract. The secondary loss is assumed a number which we vary to derive insights. Given the above, the insured firm optimally selects a deductible $x_1^*$ ( $0 \le x_1 \le b$ ) from below:

$$\underset{x_1}{Max}\begin{bmatrix} \delta\gamma\left(\int_0^{Min((x_1+G),b)} Ln(W-x-P)dx + Ln(W-x_1-P-G)(b-Min((x_1+G),b))\right) + \\ \delta(1-\gamma)\left(\int_0^{Min(x_1,b)} Ln(W-x-P-G)dx + Ln(W-x_1-P-G)(b-Min(x_1,b))\right) + \\ (1-\delta)\left(\int_0^{Min(x_1,b)} Ln(W-x-P)dx + Ln(W-x_1-P)(b-Min(x_1,b))\right) + \\ (1-q)Ln(W-P) \end{bmatrix} \tag{9}$$

Subjectto : $W > Max((G+a+P(a)),(G+b),(P(0)+Max((G,a))))$

While the above inequality constrains the minimum initial wealth of the insured firm to ensure that the argument of the logarithmic utility function remains positive, the premium structures offered by the insurer get readjusted in view of the functional forms introduced. Thus Traditional pricing premium is given as:

$$P_1 = \frac{q(1+\lambda)}{2(b-a)}(b-Max\{a,x_1\})(b+Max\{a,x_1\}-2x_1) \tag{10a}$$

Adjusted pricing premium is given as:

$$P_2 = \left\{ \begin{array}{llll} Max & \left\{ \frac{q(1+\lambda)}{2}(b+a-2x_1),\ 0 \right\} & \forall & x_1 + G < a \\ Max & \left\{ \frac{q(1+\lambda)}{2(b-a)} \left\{ (b-a)(b+a-2x_1) - \gamma\delta\left(G^2 - (a-x_1)^2\right) \right\},\ 0 \right\} & \forall\ x_1 < a, & a \le x_1 + G \le b \\ Max & \left\{ \frac{q(1+\lambda)(1-\gamma\delta)}{2}(b+a-2x_1),\ 0 \right\} & \forall\ x_1 < a\ , & x_1 + G > b \\ Max & \left\{ \frac{q(1+\lambda)}{2(b-a)} \left\{ (b-x_1)^2 - \gamma\delta G^2 \right\},\ 0 \right\} & \forall\ x_1 \ge a\ , & x_1 + G \le b \\ Max & \left\{ \frac{q(1+\lambda)(1-\gamma\delta)}{2(b-a)}(b-x_1)^2,\ 0 \right\} & \forall\ x_1 \ge a\ , & x_1 + G > b \end{array} \right\} \quad (10b)$$

Note that the bounds of search for the optimal deductible have been appropriately restricted and that the constant term $\frac{q}{b-a}$ has been omitted from the optimization. Given our uniform loss function, the upper bound of the search space for $x_1$is b: beyond that point $f(x)=0$, $F(x)=1$ everywhere, and neither the structure of expected utility $E[U]$ of the insured firm (4), nor the premium $P(x_1)$ i.e., 10(a) *or* 10(b) undergoes any change. The search range includes $a \le x_1 \le b$, because the location of $x_1$directly affects the limits of integration in the premium structure, which affects $E[U]$. Although the limits of integration in the premium structure are unaffected in $0 \le x_1 < a$ ; the premium $P(x_1)$ does change in that range because the integrand $(x - x_1)$ varies, which affects the expected utility $E[U]$ of the insured firm. In essence, the insured firm could optimally select its deductible from the range $0 \le x_1 \le b$. Since the first-order-condition of (9) is transcendental in nature, a closed form solution for optimal deductibles is difficult to establish. In what follows, we explain our numerical analysis.

The maximization problem of (9) can be construed as a set of adjacent sub problems defined by the utility and premiums for the adjacent ranges of the deductible as discussed above. The insured firm could concurrently maximize each of these sub problems to derive the corresponding optimal deductibles, and finally select the deductible that yields the highest expected utility among all the maximized solutions of the sub problems for onward communication to the insurer. The dissociation of the maximization problem into a set of sub problems is sufficient without any loss in quality of solution so long the range of deductible $0 \le x_1 \le b$ is exhaustively searched. The above process is presented in Table 3 in appendix section-3, which shows the mechanics of our numerical experiment. Every row in Table 3 represents a sub problem, which is numerically maximized twice: once under traditional pricing (*column 3*), and then under adjusted pricing (*column 4*) of premium. The process is repeated for 10 different values of each of the parameters. Appendix Section-2 provides the details of all forms of premiums and utility functions for all ranges of $a$, $b$, *and* $x_1$ and Appendix Section-3 provides the adjacent problems that are solved through the numerical experimentation.

### 5.1 Parameters and variables of experiment

We denote $W$ as the initial wealth (base value 600), which we vary 15% to study the effect of the firms wealth on the optimal deductible. The direct cyber loss $x$ is allowed to vary in a wide range, from 8% to 80% of the initial wealth. This is purposely done to include firms with widely varying operational and strategic dependence on their IT assets. The secondary loss $G$ varies from 0% to 15% of the initial wealth of the firm. At the upper range, this ratio could be construed high for large traditional firms,[9] but the deliberate choice is made to accentuate the effect of the differentiated pricing strategies between the insurer and the insured and to include the technology firms whose business may collapse altogether because of cyber breach related erosion of customer base. The probability $q$ signifies the level of security readiness of the insured firm.[10] In our experiment, we vary $q$ from 0.1 to 1.0, to the widest range of firms where some firms are almost impregnable (low $q$), and others face very high probability of breach (high $q$). The base value of the symptomatic breach $\delta$ is 0.9, signifying that systemic breaches are relatively rare. General experiences

[9] Cavusoglu et al. (2004) estimate secondary losses somewhat below 4% for the firms in their dataset.

[10] Cyber insurance providers routinely assess the security health of a prospective firm before offering a contract.

suggest infrequent systemic breaches or few attacks of pandemic nature in the current times, following criminalization of the hacker mindset.[11]

In view of the CSI/FBI surveys where up to two thirds of the respondents are reluctant to report a breach, our base value of private breach $\gamma$ is fixed at 0.7. The base market-loading factor $\lambda$ is purposely kept at a high base value 0.5 to signify the infancy of the cyber insurance market – owing to the high cost of third party security assessment and other contract writing costs. The base values and the ranges of the parameters and their symbols are tabulated in Table 2.

**Table 2** Parameters and decision variables in the numerical experiment

| Parameters and decision variables | Symbol | Base value and range |
|---|---|---|
| Secondary loss | $G$ | 50, 0 to 90 |
| Initial wealth | $W$ | 600, 600 to 690 |
| Minimum loss | $a$ | 50, 20 to 200 |
| Maximum loss | $b$ | 500, 200 to 560 |
| Conditional Probability of symptomatic breach | $\delta$ | 0.9, 0.1 to 1.0 |
| Conditional Probability of private breach | $\gamma$ | 0.7, 0.1 to 1.0 |
| Market loading factor | $\lambda$ | 0.5, 0.2 to 0.7 |
| Probability of a breach | $q$ | 0.9, 0.1 to 1.0 |

### 5.2 Results

The numerical experiment centers on (Bohme and Kataria 2006) and (Bohme and Schwartz 2010), which capture the expected utility of the insured firm and the reaction function of the insurer respectively. Recall that given the functional form of the cyber loss, it is sufficient to restrict the search for optimal deductible in $0 \le x_1 \le b$ , and that (Bohme and Kataria 2006) and (Bohme and Schwartz 2010) are already adjusted to facilitate this restricted search. The solution for the optimal deductible involves (a) separating the problem of the insured firm into a set of adjacent problems to match the premium structures for those ranges of deductible, (b) solving the adjacent problems (i.e. maximizing the expected utility of the insured firm) simultaneously for each of traditional and adjusted pricing separately, and (c) selecting the best solution from the sets of adjacent problems under each of traditional and adjusted pricing. The detailed solution procedure is presented in Appendix Section 2.

#### *5.2.1 The effect of secondary loss G on optimal deductible* $x_1^*$ and premium $P^*$

The secondary loss $G$ impacts the choice of deductible in two different ways. It works as an unmitigated background risk, which reduces the effective wealth of the insured firm; leading to higher risk aversion. Also, $G$ inflates the premium in traditional pricing (Lemma 2), thus increasing the deductible.

Between these two opposing forces, an optimal deductible is established. The opposing effects are apparent when expression (4) is investigated closely. First, the secondary loss $G$ appears in the argument of the utility function of the insured firm (approximate this effect as $W_{effective} = W - G$, a negative *wealth effect*). Here, the introduction of $G$ causes the insured firm to slide leftwards on its concave utility curve to a point where there is more risk aversion (steeper slope), and hence an incentive to buy more insurance. An increase in $G$ here works as a motivating factor to purchase more insurance, i.e., a decrease in the deductible. Second, the secondary loss $G$ also appears on the upper limit of integration and increases the range in which no indemnity payment is available. This shrinks the range of claim, and reduces the indemnity realization (*indemnity effect* of $G$). From this angle, an increase in $G$works against the motivation to purchase insurance, and increases the deductible. Unlike traditional pricing, the indemnity effect of $G$ is compensated in the premium under adjusted pricing. Thus the increase in deductible is higher for traditional pricing under the indemnity effect of $G$ (Fig. 4a).

In general, when $G$ is small, the wealth effect is smaller than the indemnity effect, and the insured firm chooses to buy less insurance (increase in the deductible). When $G$ is very small, the difference between the deductibles under traditional and adjusted pricing is insignificant, and the trajectories almost coincide (Fig. 4a). As $G$ increases further (to about 20), the premium overpricing effect starts to dominate (see proof of Lemma 2: a quadratic increase occurs in the range $G < b - x_1^*$ ). Now the trajectory of the optimal deductible under traditional pricing ($x_{11}^*$ ) visibly rises above that under adjusted pricing ($x_{12}^*$ ); this trend accelerates till $G = b - x_1^*$. After that, the overpricing remains constant (see proof of Lemma 2), and the trajectories of $x_{11}^*$ and $x_{12}^*$ are about parallel.

At a high value of $G$, the negative wealth effect is more significant. The insured firm is more risk averse and is ready to buy more insurance (lower deductible). This arrests the rising trend of deductible, before bringing in a decreasing trend. As the deductible decreases, the insured firm regains its ability to claim private symptomatic breaches, and the decreasing trend sustains.

The trend of the trajectories of $P_1^*$ and $P_2^*$ reflects the movement of the deductibles $x_{11}^*$ and $x_{12}^*$. For example, at small levels of $G$, we find a decreasing trend in premiums, whereas at high levels of $G$, the premiums (Fig. 4b) increase with $G$.

[11] More of the perpetrators of current computer crime are motivated by money, not bragging rights (CSI survey, 2007).

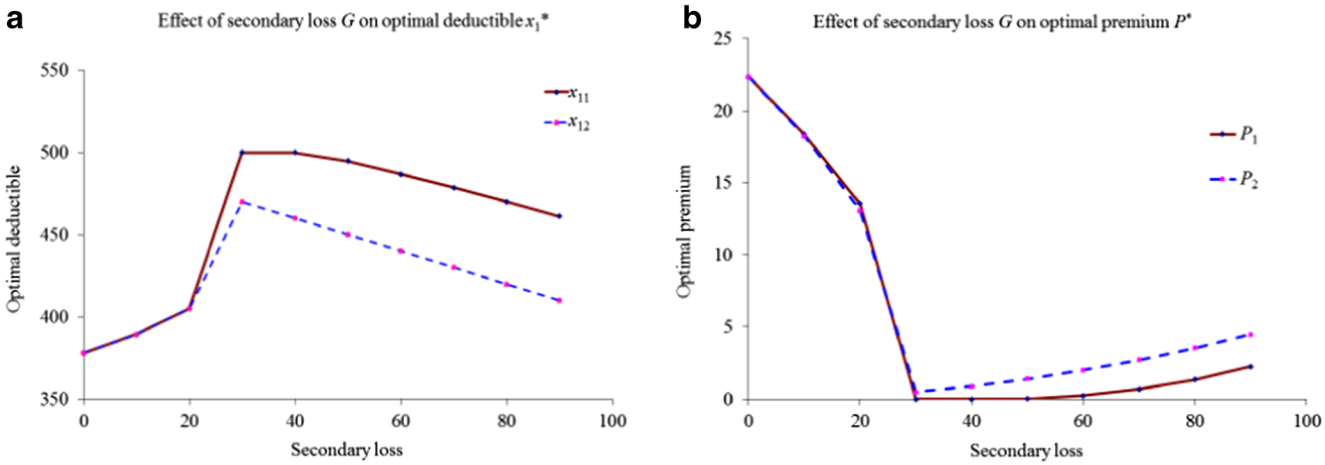



**Fig. 4** Effect of secondary loss G on optimal deductible and premium

Because there is no premium overpricing in adjusted pricing, the increasing trend of $P_2^*$ for high and increasing $G$ is purely attributable to the decreasing deductible.

### 5.2.2 Effect of private breach $\gamma$on optimal deductible $x_1^*$ and premium $P*$

When $\gamma$ rises for fixed $G$, there is no immediate effect in the no-claim range. However, as $\gamma$ increases, losses ($\forall x < (x_1 + G)$) in private breaches remain unclaimed with higher frequency. This incentivizes the insured firm to reduce the deductible (ideally for symptomatic breaches - if this were possible, which is not) such that the effective claiming range can be increased. On the other hand an increase in $\gamma$- i.e., a decrease in ( $1-\gamma$), decreases the frequency of claim for a public breach, making it amenable for an increase in the deductible for public breaches alone - if it were possible - to gain on the reduced premium. However, cyber insurance contracts require a unique deductible, and the expected utility of the insured firm, in a sense, is the weighted average of the expected utilities of private and public breaches.

When $\gamma$ is small, the tendency to increase the deductible for public breaches dominates over the need to decrease the deductible for private breaches. Hence, the overall effect at small values of increasing $\gamma$on the deductible is a net increasing trend. However as $\gamma$ increases further, the decision suitable for the private breaches gains more significance and the rate of increase in the deductible starts decreasing till it is finally arrested (Fig. 5a). The premiums fall as a reaction to the selection of the deductible by the insured firm, and the rate of fall in both $P_1^*$ and $P_2^*$ is increasingly flatter at higher levels of $\gamma$ because $\frac{dP}{dx_1}$ flattens out at elevated levels of $x_1^*$. Note that the cyber insurance contract stops selling under traditional pricing beyond $\gamma = 0.65$ in the model of experimentation; $P_1^* = 0$ voids a contract by definition (Fig. 5b)

### 5.2.3 Firm wealth W, intensity of IT operations k, and optimal deductible$x_1^*$

Insight from insurance economics suggests that higher levels of wealth make smaller losses appear insignificant, and wealthier firms find it optimal to insure only large and catastrophic losses. However, there is no understanding how the size of a firm $W$and the secondary losses $G$ correlate in the purchase of cyber insurance.

To analyze this, we introduce $k = \frac{G}{W}$ i.e., the secondary loss as a proportion of the firm size (wealth) and use this factor as a surrogate for the *relative intensity of IT* for the firm. If $W$ increases keeping $k$ constant, $W-G$ increases, suggesting an increase in deductible (wealth effect). However, note that $G$ must also rise implicitly with $W$ in order to keep the ratio $k$ fixed, which in turn suggests a decrease in deductible (Fig. 4a). These opposing effects are roughly balanced, and the constant $k$ curves are quite flat (Fig. 6a and b). It is interesting to note that firms with similar IT intensity buy similar amounts of cyber insurance - an intuitive outcome. When $k$ is allowed to increase (more IT intensive operations), higher rise in $G$ is established. As a result, the (reducing) wealth effect now dominates, which reduces the deductible. The equilibrium premiums follow directly from the deductibles and are not separately presented here.

### 5.2.4 Performance of cyber insurance contract under the two different pricing strategies

We can compare the relative performances of a cyber insurance contract in transferring IT risk between the traditional and adjusted pricing by comparing the levels of optimal deductibles. For example, a positive value of ($x_{11}^* - x_{12}^*$ ) implies

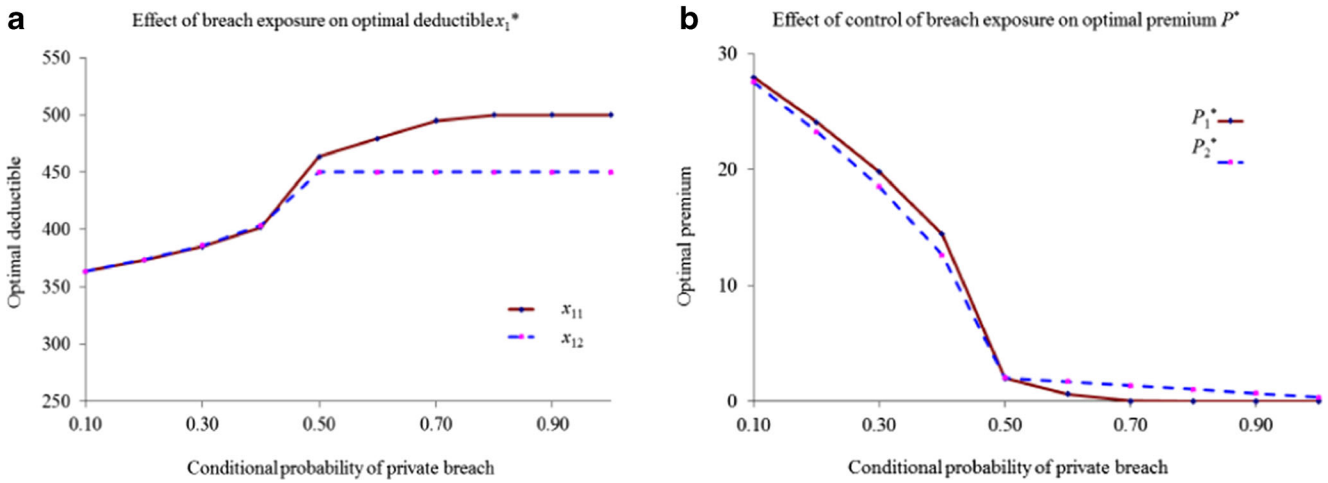



**Fig. 5** Effect of private breach exposure on optimal deductible $x_1^*$ and Premium $P^*$

that the contract optimally transfers more IT risk under adjusted pricing. Here we investigate the changes in risk transfer as $k$, $G$ and $\gamma$ change. As $k$ is allowed to increase (also implies an increase in $G$) with the increase in $W$, in order to recover part of the lost claiming range in private breach, and also as a reaction to the (reducing) wealth effect, both $x_{11}^*$ and $x_{12}^*$ fall in traditional and adjusted pricing.

However, the overall level of $(x_{11}^*-x_{12}^*)$ exhibits rising trend because reducing deductible is cheaper in adjusted pricing (Fig. 7), denoting higher levels of risk transfer under adjusted pricing as $k$increases. On the other hand, increasing $W$at constant $k$ has a net positive wealth effect, i.e., ($W-G$ monotonically rises) in both traditional and adjusted pricing. As a result $x_{11}^*$ and $x_{12}^*$ both rise. Although the contract transfers more risk under adjusted pricing now, the difference in risk transfer remains virtually constant between traditional and adjusted pricing (Fig. 7).

For constant $W$, the wealth effect $G$ is invariant between traditional and adjusted pricing, and keeps on increasing with $G$. On the other hand, as $G$ increases from small values, the decrease in claim range in traditional pricing rises steadily and increases the deductible$x_{11}^*$, which increases$x_{11}^*-x_{12}^*$. Such monotonic trend however slows down as the (reducing) wealth effect of $G$ catches up and begins to preponderate (see Fig. 4), which arrests the rise of $x_{11}^*-x_{12}^*$ and flattens the curve at higher value of $G$.

For small values of $\gamma$, when $\gamma$ increases (see Fig. 5a), there is little gain in risk transfer between the scenarios of traditional and adjusted pricing since reduced frequency in claiming private breaches ($\forall\ x<x_1+G$), being low, has little effect on the deductibles. The initial rate of rise in $x_{12}^*$ falls below that of $x_{11}^*$ (see Fig. 5a), and $(x_{11}^*-x_{12}^*)$ rises fast in the mid-range of $\gamma$. Finally, the rates of rise of $x_{12}^*$ and $x_{11}^*$ both trail off, and the increase in risk transfer remains constant at high levels of $\gamma$. In the mid to high range of $\gamma$, the contract thus transfers significantly higher risk under adjusted pricing (Fig. 7).

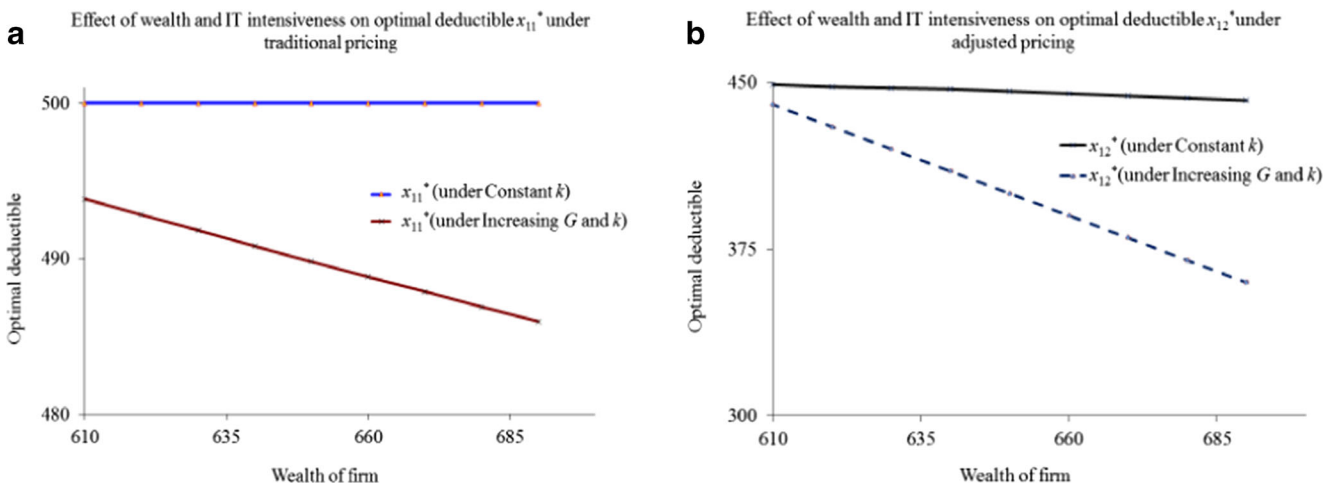



**Fig. 6** Effect of firm wealth and IT intensiveness on optimal deductible under traditional/adjusted pricing

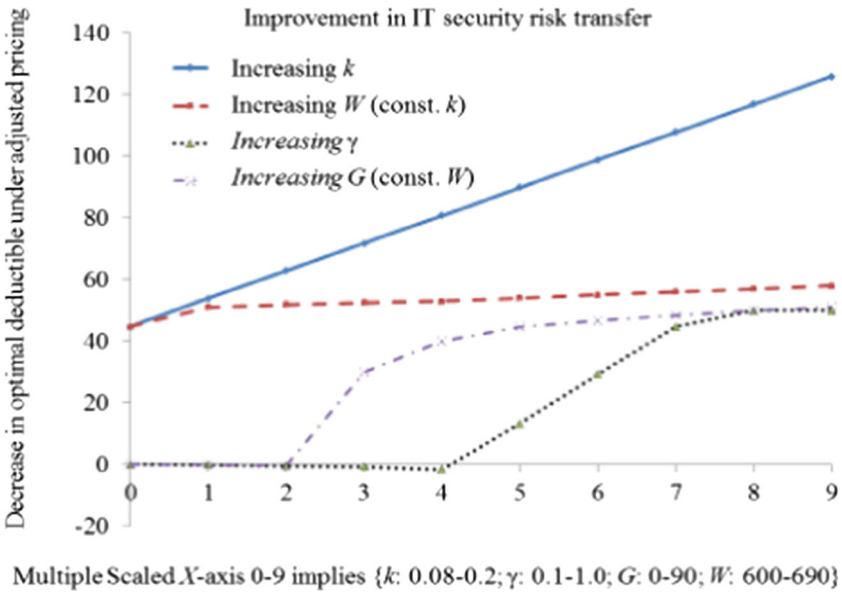



**Fig. 7** Increased risk transfer under adjusted pricing

*5.2.5 The value of cyber insurance to the contracting parties*

The previous subsection shows that when $x_{11}^* - x_{12}^* \geq 0$, the contract optimally transfers higher risk under adjusted pricing than otherwise and thus is a desirable market outcome. However, the net value of the contract to the parties are reflected in their payoffs. Let the expected utility of the risk averse insured firm in traditional (adjusted) pricing be $U_1^* = U_1(x_{11}^*)$ ( $U_2^* = U_2(x_{12}^*)$ ). The insurer is risk neutral, its payoff in traditional (adjusted) pricing be $\Pi_1^*(\Pi_2^*)$. Under traditional pricing, the insurer receives $P_1(x_{11}^*)$ as the upfront payment but actually pays out $\frac{P_2(x_{11}^*)}{(1+\lambda)}$ as indemnity. This happens because the traditional contract is offered without any consideration of $G$ and $\gamma$ (unadjusted pricing), but the post contract operationalization cannot be immune to the realized scenarios of IT security breaches. As a result, under traditional pricing. $\Pi_1^* = P_1(x_{11}^*) - \frac{P_2(x_{11}^*)}{(1+\lambda)}$, and under adjusted pricing $\Pi_2^* = P_2(x_{12}^*) - \frac{P_2(x_{12}^*)}{(1+\lambda)}$. Thus a *positive* $\Delta U = U_2^* - U_1^*$ ( $\Delta\Pi = \Pi_2^* - \Pi_1^*$ ) represent an increase in utility of the insured (insurer) when the market moves from traditional to adjusted pricing.

The incremental gains (losses) in utility of the contracting parties are presented in Fig. 8a and b. Note that the insured firm is always better off under adjusted pricing ( $U_2^* - U_1^* \geq 0$ ). The same however, is not necessarily true for the insurer as we explain it below.

When $G$ is small (up to 20 or so) the deductibles between the two different pricings are almost equal (Fig. 5a), and the static effect of premium overpricing (Lemma-2) alone increases the utility of the insurer under traditional pricing. In the higher range of $G$, the insured firm increasingly forfeits more of its indemnity receipts from the symptomatic private breaches because of its strategic *underclaiming behavior* under traditional pricing, which in turn results in lower amount of insurance purchase. Thus when $G$ is high, the deductible is much lower under adjusted pricing, and the insurer is better off from a higher stream of premium.

The effect of increasing $\gamma$ on the relative improvement of the utility of the insurer in adjusted pricing is not monotonic. For small values of $\gamma$, when $\gamma$ increases, there is small gain in risk transfer ($x_{11}^* - x_{12}^*$ is small) between the scenarios of traditional and adjusted pricing (Fig. 5a). This small increase in uptake of insurance however does not compensate the loss of excessive rent that the insurer was able to extract under unadjusted pricing. As a result, the utility of the insurer initially falls. However, at moderate to high levels of $\gamma$ (begins at about 0.3), the increased uptake of insurance in adjusted pricing regime begins to compensate the loss of excessive rent that the insurer was able to extract under unadjusted pricing. Now the trend reverses and the insurer breaks even at about $\gamma = 0.4$, beyond which an increase in utility under adjusted pricing is ensured for the insurer.

Under increasing $W$, an insured firm buys less insurance (wealth effect); but in adjusted pricing, the insured firm buys relatively more insurance, and the utility of the insurer improves from a higher stream of premium payment. Firms with Higher IT intensive operations (higher $k$) buy more insurance in adjusted pricing and the insurer is better off from a higher stream of premiums as well (Fig. 8b).

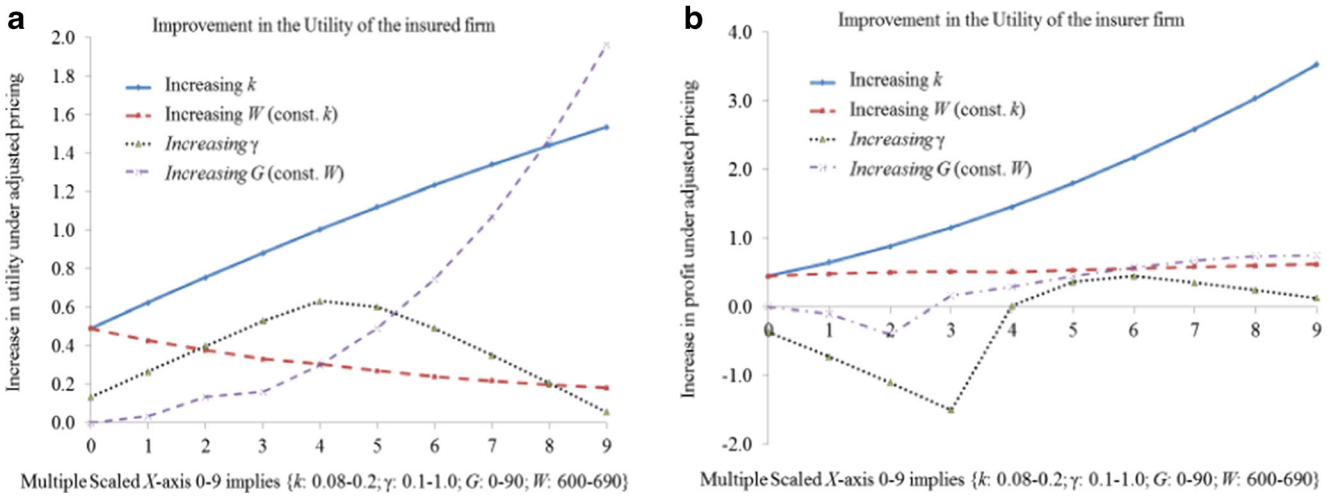



**Fig. 8** Changes in the expected utility of the Insurer and Insured between traditional and adjusted pricing

## 6 Discussion

Having assembled and analyzed the cyber insurance utilization model, we now discuss and connect the impact of secondary losses with observations from cyber insurance market.

If a firm faces no secondary loss, the contracted and operationalized deductibles coincide, and the insured firm optimally exhibits the contract-intended behavior. This case is no different than the standard scenario in a developed traditional insurance market. However, this is an unlikely scenario in present time. Secondary losses including reputational losses are some of the commonly accepted losses from cyber breaches now (Betterly Report 2015). Optimal operationalization of a cyber insurance policy can also coincide with the contract-intended behavior when the insurer appropriately adjusts the plausible underclaiming behavior of the insured firm caused by distributed breaches that selectively accrues secondary losses. However, there are complicating factors in this. The deviations from the contract intended behavior can occur for multiple reasons. First, in presence of secondary loss $G$, symptomatic private breaches in the range between the contracted deductible $x_1$ and $r = x_1 + G$ can remain unclaimed. This happens because higher secondary loss $G$ increases the difference between $x_1$ and $r$ (Fig. 3). Second, a higher proportion of symptomatic private breach $\gamma$ raises the frequency with which the off contract claiming behavior is optimal. When this happens, the de-facto deductible $r$ and not the contracted deductible $x_1$ is operationalized more frequently while making actual claims (Fig. 3). Third, the insurer may altogether avoid adjusting the pricing structure if that does not correspond to its own optimal premium intake. Finally, the realization of breaches in terms of the types and frequencies remain stochastic, and claiming is strictly an ex-post breach decision. Thus, in absence of large amount of indemnity payout data,[12] insurers are conservative in their approach while writing contracts. This results in low limits of covered losses, high premium and myriad exclusions of breach events in cyber insurance products and contracts (Schroeder 2014[13]).

It is possible to use our results to explain the cyber insurance market dynamics:

In the nineties, the market for cyber insurance might have begun in an immature manner when neither the insured nor the insurer was specifically aware of $G$ and $\gamma$. The cyber risks and their natures were barely understood at that point in time. As a result, few cyber insurance contracts were written with experiences from traditional products and established insurance markets.

Research studies like Cavusoglu et al. (2004)and other market evidences in the 2000s made it clear that firms may suffer secondary losses following primary cyber losses, as stakeholders adversely reassess the post-breach IT security health of the firms. This realization caused the insured firms to formalize an optimized claiming strategy, which differed from the contract-intended behavior under the traditional or unadjusted premium pricing structure. Under this situation, a lower amount of IT risk was optimally transferred (Fig. 7), and the contract was overpriced for a given deductible (Lemma 1 and 2) reducing the general appeal of cyber insurance. This may explain why so little cyber insurance – just about 150 million dollars or so (Betterly Report, 2010) was sold till the year 2009.

Industry analysis (for example, see Ponemon Studies 2008 and 2015; and Verizon Data Breach Investigation Report,

[12] for some small scale analysis of indemnity payout in cyber insurance, please refer to the 2011 and 2012 reports from Netdiligence Inc. at http://netdiligence.com/files/CyberLiability-0711sh.pdf and http://www.resultstechnology.com/files/2013/05/2012-10-Cyber-Claims-Study.pdf

[13] http://blogs.wsj.com/cio/2014/03/27/cyber-insurance-just-one-component-of-risk-management/

2015) consistently suggest that as hackers have evolved into financial mercenaries, average breach costs have consistently increased over time ($5.4 million in 2014 as against $4.5 million in 2013). These studies also suggest that breaches are often attributable to organizational failures to protect their information assets from predictable patterns of cyberattacks. In this connection it is appropriate to recall the case of TJMax failure, where an available security patch was not deployed in a timely manner and contrary to industry practices, stored consumer data was not encrypted! The above industry analyses allude to high impact breaches and elevated proportion of symptomatic breaches in the mix, which are equivalent to high and increasing $G$ and $\gamma$ in our study. Parallel analysis of our model under these circumstances shows that the insurer is increasingly better off under adjusted pricing (Fig. 8b). Under the *adjusted* premium structure, this also makes the cyber insurance contract more amenable for the insured firm as premium overpricing trails off. Together, these help explain the recent growth in the cyber insurance market, which has now reached a decent size of 2.5 billion dollars in 2015 (Betterly report 2015).

Firms with low $G$, or firms under regulatory obligations for disclosure are more likely to buy cyber insurance than otherwise. When regulation framework becomes comprehensive (which is equivalent to a low proportion of private breaches in our model), the contract becomes equitably priced and is more amenable for adoption by the insured firm. There appears to be another small segment of firms who use cyber insurance for strategic and competitive posture.[14] These firms buy cyber insurance to assure their stakeholders, but choose very high deductible with no serious intention or possibility to ever reclaim normal mid-range cyber losses. Equivalently, in our framework also, a firm with high $G$ chooses high deductible as an ad-hoc strategy, because a higher ratio of $x_1$ to $G$ ($r = x_1 + G$) tends to offset the relative overpricing of the contract.

Although occurrence of secondary losses has been empirically confirmed, the exact nature of these losses is not known. We do not foresee major changes in the results from our model when other functional forms of secondary loss are substituted for the constant secondary loss that we have used in the experiment. For further exposition, we have investigated a firm"s claim strategy for a claim dependent convex loss (Appendix Section 4). The results indicate that similar overpricing effects may exist there too.

## 7 Concluding Remarks

In this work, we have explored different types of breaches and comprehensively characterized them to model losses from those differentiated breaches to arrive at the practical circumstance of utilization of a cyber insurance contract. Having done so, we have analyzed a set of 3 simplified cases and derived closed form solutions to demonstrate multiple optimal pricings that denote plausible but opposing postures of the insurers in their appreciation of secondary losses while they structure the financial instruments of cyber insurance. We have carried out extensive experimentation with the full model to derive insights of the impact of secondary loss on the efficiency and efficacy of such instruments in transferring residual cyber risk to the market. We have also indicated those firm and market factors which could make cyber insurance products more efficient and less expensive and can stimulate increased use.

As evident from industry press, the circumstances of cyber insurance consumption are complex. Detecting, understanding, assessing, estimating and claiming a realized breach faces great deal of challenges.

IT security breaches are significantly different from physical breaches. Unlike a physical breach, a data breach may remain unnoticed for a very long time - the TJMax breach continued for about 14 months before the management conclusively determined and sealed the breach. Even if a breach is detected, the losses are difficult to assess - an unauthorized copy from a restricted dataset does not destroy the original, and a random act of garbling a dataset is not easily discerned. Many tell-tale signs of breach are confused with production issues - bandwidth/server hijacking may be confused with heightened traffic volume – making actionable feedback on unfolding incidents difficult.

The management of IT security breaches is complex and involved. Breach investigation and assessment of losses may not get priority for breaches, only recovery efforts predominate to control losses and reputational damages and bring the systems back to service. Often a breach is not reported to the authorities, fearing that the IT assets could be labeled as evidence of crime and decommissioned for long periods of time. Even when authorities are informed, inexperienced pre-handling of breach incidence often causes loss of evidences and traces of cybercrime. Finally, third party liabilities arise quite late since establishing a connection of liability with the breach rests on the injured.

The administration of cyber insurance contract is distributed and confusing, which demands cross functional knowledge. Current practice of implementing cyber insurance contracts requires sound understanding of both IT and traditional risk management, which the IT manager may not possess. For example, it is not intuitive to realize that a physical damage to an employees laptop is differently covered through traditional insurance contracts, yet a lost laptop may be covered in a cyber insurance contract! On the other hand, the traditional risk managers are not knowledgeable about IT breaches and cyber risks, and a knowledge gap exists between the IT and risk management functions hindering the seamless collaboration needed for integrating cyber insurance in the enterprise risk management paradigm.

The current cyber insurance products in the market are offered in 4 areas of losses, viz., Errors and Omissions, Media Liability,

[14] Based on our private communications on the value of cyber insurance with CIOs/CISOs.

Network Security, and Privacy (Floresca 2014). On the other hand, the breaches are analyzed at the intersections of *architecture* (e.g., network/server breach), *information asset* (e.g., data breach), or *attack vector* (e.g., virus and worms) in the consumption end. Since similar losses can emanate from multiple types of breaches e.g., privacy loss can occur both from network breach as well as from malware download, understanding cyber insurance coverages and making appropriate claiming decisions is complex, which IT/IS managers may avoid, especially for smaller losses. Currently offered cyber insurance products specifically exclude secondary losses (e.g., reputational and goodwill losses, loss from customer churn etc.) which however stubbornly remain attendant to primary losses when stakeholders come to know of realized breaches.

With time, when the insurance industry collects substantial historical claim data to make actuarially fair estimations on stochastic distributions of indemnity payments, the paradigm would likely coincide with the appropriately adjusted pricing structure (similar to the one that we have modeled and analyzed). We conjecture that passage of time will also help address the knowledge gap that currently exists between the risk managers and the IT managers, making firms more comfortable with the integral use of cyber insurance products in risk management.

## Appendices for a model to analyze the challenge of using cyber insurance

### Appendix Section 1: Proof of proposition-1, Lemma-1, and Lemma-2

**Proposition 1** *For a secondary loss Gassociated with a realized private symptomatic breach, there exists a minimum realized loss* $r$ $(=x_1+G)$ *up to which the insured firm does not claim its losses, for losses above r, the insured firm claims its actual loss.*

*Proof* The local optimization problem is reduced to locate an arbitrary point $r$ in the loss axis (Fig. 4) such that the expected net revenue from the payout $E[R(r)] = \int_r^{\infty} I(x)f(x)dx - (1-F(r))$ is maximized. The FOC of the above yields the optimal$r$: $r=I^{-1}(G)$. However, the point $r$ must lie towards the right of point$x_1$ (the firm has no reason to claim below the deductible and absorb just the secondary losses). Thus in general: $r=I^{-1}(r-x_1)$. This fixes the point $r$-conclusively, $r=x_1+G$. The point $r$ marks the boundary, beyond which the insured firm claims a suffered loss in the private breach.

**Lemma 1** *For any given deductible, the premium structure under adjusted pricing is never higher than that under traditional pricing* i.e. $P_1(x_1)\geq P_2(x_1)$

*Proof* It can be shown that$P_2 = P_1 - q(1+\lambda)\gamma\delta\int_{x_1}^{x_1+G}(x-x_1)f(x)\,dx$, such that for nonnegative values for $G$, $\delta$, $\gamma$, and $\lambda$, $P_1 \geq P_2$.

**Lemma 2** *For a selected deductible* $x_1$, $x_1 \geq 0$, *overpricing* $(P_1 - P_2)$ *under traditional pricing:*

1) *Increases linearly with the probability of private breach* $\gamma$
2) *Increases non-linearly with the expected secondary loss* $G$

*Proof* The overpricing is denoted as $\Delta P = q(1+\lambda)\gamma\delta\int_{x_1}^{x_1+G}(x-x_1)\,f(x)\,dx$. Under our uniform primary loss distribution assumptions with range $[a, b]$, these salient cases follow:

$$\text{Case-1}: \Delta P = q(1+\lambda)\gamma\delta\int_{x_1}^{x_1+G}(x-x_1)\,0\,dx = 0, \qquad x_1+G<a$$

$$\text{Case-2}: \Delta P = q(1+\lambda)\gamma\delta\int_{a}^{x_1+G}(x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)\gamma\delta}{2(b-a)}\left(G^2-(a-x_1)^2\right), \qquad x_1<a,\quad a\leq x_1+G\leq b$$

$$\text{Case-3}: \Delta P = q(1+\lambda)\gamma\delta\int_{a}^{b}(x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)\gamma\delta}{2}(b+a-2x_1), \qquad x_1<a,\quad x_1+G>b$$

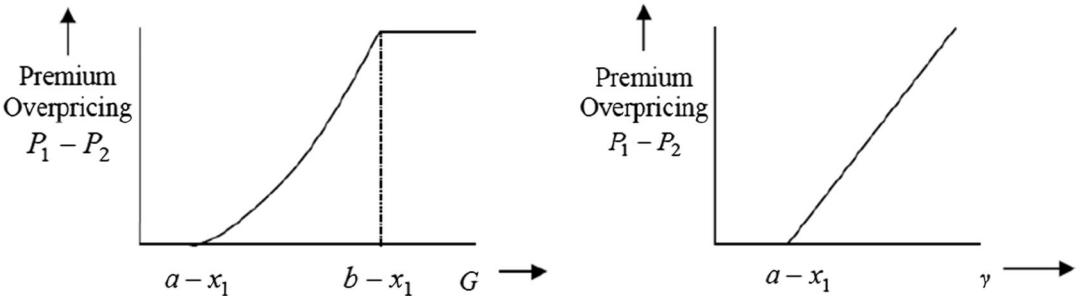
$$\text{Case-4}: \Delta P = q(1+\lambda)\gamma\delta\int_{x_1}^{x_1+G}(x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)\gamma\delta}{2(b-a)}G^2, \qquad a\leq x_1\leq b,\quad a\leq x_1+G\leq b$$

$$\text{Case-5}: \Delta P = q(1+\lambda)\gamma\delta\int_{x_1}^{b}(x-x_1)\frac{1}{b-a}\,dx = \frac{q(1+\lambda)\gamma\delta}{2(b-a)}(b-x_1)^2, \qquad a\leq x_1\leq b,\quad x_1+G>b$$

*As a result, the overpricing of Premium exhibits the following characteristics (diagram below)*

- Does not exist in the range $x_1 \leq Max\{(a-G),0\}$
- Increases linearly with the probability of private breach $\gamma$ in the range$x_1 > Max\{(a-G),0\}$
- Exhibits quadratic increase with the secondary loss G in the range $a < x_1+G \leq b$

- Remains invariant of the secondary loss G in the range $x_1 > Max\{(b-G),\ 0\}$




**Appendix Section 2: Derivation of utility and premium expressions**

*A. Derivation of the offered premiums in the given ranges of deductible:*

*Scenario-1, Unadjusted:*

$$\text{Case } 1: P_1 = q(1+\lambda)\int_a^b (x-x_1)\frac{1}{b-a}dx = \frac{q(1+\lambda)}{2}(b+a-2x_1) \qquad x_1 < a$$

$$\text{Case } 2: P_1 = q(1+\lambda)\int_{x_1}^b (x-x_1)\frac{1}{b-a}dx = \frac{q(1+\lambda)}{2(b-a)}(b-x_1)^2 \qquad x_1 \geq a$$

$$\text{Thus in general}: P_1 = \frac{q(1+\lambda)}{2(b-a)}(b-Max\{a,x_1\})(b+Max\{a,x_1\}-2x_1)$$

*Scenario-2, Adjusted:*

$$\text{Case}-1: P_2 = q(1+\lambda)\left\{\int_a^b (x-x_1)\frac{1}{b-a}dx - \gamma\delta\int_{x_1}^{x_1+G}(x-x_1).0.dx\right\} \qquad \forall\ x_1+G < a$$

$$P_2 = Max\left\{\frac{q(1+\lambda)}{2}(b+a-2x_1),\ 0\right\} \qquad \forall\ x_1+G < a$$

$$\text{Case}-2: P_2 = q(1+\lambda)\left\{\int_a^b (x-x_1)\frac{1}{b-a}dx - \gamma\delta\int_a^{x_1+G}(x-x_1).\frac{1}{b-a}.dx\right\} \qquad \forall\ x_1 < a,\quad a \leq x_1+G \leq b$$

$$P_2 = Max\left\{\frac{q(1+\lambda)}{2(b-a)}\left\{(b-a)(b+a-2x_1) - \gamma\delta\left(G^2-(a-x_1)^2\right)\right\},\ 0\right\} \qquad \forall\ x_1 < a,\quad a \leq x_1+G \leq b$$

$$\text{Case}-3: P_2 = q(1+\lambda)\left\{\int_a^b (x-x_1)\frac{1}{b-a}dx - \gamma\delta\int_a^b (x-x_1).\frac{1}{b-a}.dx\right\} \qquad \forall\ x_1 < a,\quad x_1+G > b$$

$$P_2 = Max\left\{\frac{q(1+\lambda)(1-\gamma\delta)}{2}(b+a-2x_1),\ 0\right\} \qquad \forall\ x_1 < a,\quad x_1+G > b$$

$$\text{Case}-4: P_2 = q(1+\lambda)\left\{\int_{x_1}^b (x-x_1)\frac{1}{b-a}dx - \gamma\delta\int_{x_1}^{x_1+G}(x-x_1).\frac{1}{b-a}.dx\right\} \qquad \forall\ x_1 \geq a,\quad x_1+G \leq b$$

$$P_2 = Max\left\{\frac{q(1+\lambda)}{2(b-a)}\left\{(b-x_1)^2 - \gamma\delta G^2\right\},\ 0\right\} \qquad \forall\ x_1 \geq a,\quad x_1+G \leq b$$

$$\text{Case}-5: P_2 = q(1+\lambda)\left\{\int_{x_1}^b (x-x_1)\frac{1}{b-a}dx - \gamma\delta\int_{x_1}^b (x-x_1).\frac{1}{b-a}.dx\right\} \qquad \forall\ x_1 \geq a,\quad x_1+G > b$$

$$P_2 = Max\left\{\frac{q(1+\lambda)(1-\gamma\delta)}{2(b-a)}(b-x_{''s1})^2,\ 0\right\} \qquad \forall\ x_1 \geq a,\quad x_1+G > b$$

B: Derivation of the expected utility of the insured firm, in the given ranges of deductible

| Range of $x_1$ | Range Adjusted Expected Utility of the insured firm $E[U]$ ($P = P_1$ or $P_2$ from above as the case may be) |
|---|---|
| General form | $q\delta\gamma\left(\int_0^{x_1+G} U(W-x-P)f(x)dx + U(W-x_1-P-G).(1-F(x_1+G))\right) + q\delta(1-\gamma)\left(\int_0^{x_1} U(W-x-P-G)f(x)dx + U(W-x_1-P-G).(1-F(x_1))\right) + q(1-\delta)\left(\int_0^{x_1} U(W-x-P)f(x)dx + U(W-x_1-P).(1-F(x_1))\right) + (1-q).U(W-P)$ |
| Utilizing Functional form, and $x_1+G<a$ | $q\delta\gamma\left(Ln(W-x_1-P-G).1\right) + q\delta(1-\gamma)\left(Ln(W-x_1-P-G).1\right) + q(1-\delta)\left(Ln(W-x_1-P).1\right) + (1-q)Ln(W-P)$ <br> $=$ <br> $q\delta.Ln(W-x_1-P-G) + q.(1-\delta).Ln(W-x_1-P) + (1-q).Ln(W-P)$ |
| Utilizing Functional form, and $x_1<a$, $a\le x_1+G$ | $q\delta\gamma\left(\int_a^{x_1+G} Ln(W-x-P)\frac{1}{b-a}dx + Ln(W-x_1-P-G).\frac{(b-x_1-G)}{b-a}\right) + q\delta(1-\gamma)\,Ln(W-x_1-P-G) + q(1-\delta)\,Ln(W-X_1-P) + (1-q).U(W-P)$ <br> $=$ <br> $\frac{q\delta\gamma}{b-a}.\left((W-a-P).Ln(W-a-P) - (W-b-P).Ln(W-x_1-P-G) - (x_1+G-a)\right) + q\delta(1-\gamma).Ln(W-x_1-P-G) + q.(1-\delta).Ln(W-x_1-P) + (1-q).Ln(W-P)$ |
| Utilizing Functional form, and $x_1<a$, $x_1+G>b$ | $q\delta\gamma\left(\int_a^{b} Ln(W-x-P)\frac{1}{b-a}dx + 0\right) + q\delta(1-\gamma)\,Ln(W-x_1-P-G) + q(1-\delta)\,Ln(W-X_1-P) + (1-q).U(W-P)$ <br> $=$ <br> $\frac{q\delta\gamma}{b-a}.\left((W-a-P-G).Ln(W-a-P-G) - (W-b-P-G).Ln(W-b-P-G) - (x_1-a)\right) + q\delta(1-\gamma).Ln(W-x_1-P-G) + q.(1-\delta).Ln(W-x_1-P) + (1-q).Ln(W-P)$ |
| Utilizing Functional form, and $x_1\ge a$, $x_1+G\le b$ | $q\delta\gamma\left(\int_a^{x_1+G} Ln(W-x-P)\frac{1}{b-a}dx + Ln(W-x_1-P-G)\frac{b-x_1-G}{b-a}\right) + q\delta(1-\gamma)\left(\int_a^{x_1} Ln(W-x-P-G)\frac{1}{b-a}dx + Ln(W-x_1-P-G).\frac{b-x_1}{b-a}\right) + q(1-\delta)\left(\int_a^{x_1} Ln(W-x-P)\frac{1}{b-a}dx + Ln(W-x_1-P).\frac{b-x_1}{b-a}\right) + (1-q).Ln(W-P)$ <br> $=$ <br> $\frac{q\delta\gamma}{b-a}.\left((W-a-P).Ln(W-a-P) - (W-b-P).Ln(W-x_1-P-G) - (x_1+G-a)\right) + \frac{q\delta(1-\gamma)}{b-a}.\left((W-a-P-G).Ln(W-a-P-G) - (W-b-P-G).Ln(W-x_1-P-G) - (x_1-a)\right) + \frac{q(1-\delta)}{b-a}.\left((W-a-P).Ln(W-a-P) - (W-b-P).Ln(W-x_1-P) - (x_1-a)\right) + (1-q).Ln(W-P)$ |
| Utilizing Functional form, and $x_1\ge a$, $x_1+G>b$ | $q\delta\gamma\left(\int_a^{b} Ln(W-x-P)\frac{1}{b-a}dx + 0\right) + q\delta(1-\gamma)\left(\int_a^{x_1} Ln(W-x-P-G)\frac{1}{b-a}dx + Ln(W-x_1-P-G).\frac{b-x_1}{b-a}\right) + q(1-\delta)\left(\int_a^{x_1} Ln(W-x-P)\frac{1}{b-a}dx + Ln(W-x_1-P).\frac{b-x_1}{b-a}\right) + (1-q).U(W-P)$ <br> $=$ <br> $\frac{q\delta\gamma}{b-a}.\left((W-a-P).Ln(W-a-P) - (W-b-P).Ln(W-b-P) - (b-a)\right) + \frac{q\delta(1-\gamma)}{b-a}.\left((W-a-P-G).Ln(W-a-P-G) - (W-b-P-G).Ln(W-x_1-P-G) - (x_1-a)\right) + \frac{q(1-\delta)}{b-a}.\left((W-a-P).Ln(W-a-P) - (W-b-P).Ln(W-x_1-P) - (x_1-a)\right) + (1-q).Ln(W-P)$ |

## Appendix Section 3: Adjacent problems for the experiment - solution procedure

The maximization problem of (9) can be construed as a set of adjacent sub problems defined by the pertinent ranges of the deductible. The insured firm could concurrently maximize each of these sub problems to derive the corresponding optimal deductibles, each of which is now specific to the deductible range. Finally, among all these range-specific optimal deductibles, the deductible that yields the highest expected utility among all the maximized solutions of the sub problems could then be selected for onward communication to the insurer. The dissociation of the maximization problem into a set of sub problems is sufficient without any loss in quality of solution so long the restricted range of deductible $0 \le x_1 \le b$ is exhaustively searched. The above process is represented in the following table, which is how we conduct our numerical experiment. Every row in Table 3 represents a sub problem, which is numerically maximized twice: once under traditional pricing (*column 3*), and then under adjusted pricing (*column 4*) of premium. The process is repeated for 10 different values of each of the parameters.

**Table 3** Sub problems of expected utility maximization under traditional and adjusted premiums

| Range of deductible $x_1$ | Expected Utility of the insured $E[U]$ | Premium in traditional pricing $P_1$ | Premium in adjusted pricing $P_2$ |
|---|---|---|---|
| $x_1 + G < a$ | $q\delta.Ln(W-x_1-P-G)+ q.(1-\delta).Ln(W-x_1-P) + (1-q).Ln(W-P)$ | $\frac{q(1+\lambda)}{2}(b + a-2x_1)$ | $Max\left\{\frac{q(1+\lambda)}{2}(b + a-2x_1),\ 0\right\}$ |
| $x_1 < a,$ $a \le x_1 + G$ | $\frac{q\delta\gamma}{b-a}.\begin{pmatrix}(W-a-P).Ln(W-a-P)-\\(W-b-P).Ln(W-x_1-P-G)-(x_1+G-a)\end{pmatrix}$ $+q\delta(1-\gamma).Ln(W-x_1-P-G) + q.(1-\delta).Ln(W-x_1-P)$ $+(1-q).Ln(W-P)$ | $\frac{q(1+\lambda)}{2}(b + a-2x_1)$ | $Max\left\{\frac{q(1+\lambda)}{2(b-a)}\begin{Bmatrix}(b-a)(b + a-2x_1)-\\ \gamma\delta\left(G^2-(a-x_1)^2\right)\end{Bmatrix},\ 0\right\}$ |
| $x_1 < a,$ $x_1 + G > b$ | $\frac{q\delta\gamma}{b-a}.\begin{pmatrix}(W-a-P-G).Ln(W-a-P-G)-\\(W-b-P-G).Ln(W-b-P-G)-(x_1-a)\end{pmatrix}+$ $q\delta(1-\gamma).Ln(W-x_1-P-G) + q.(1-\delta).Ln(W-x_1-P)+$ $(1-q).Ln(W-P)$ | $\frac{q(1+\lambda)}{2}(b + a-2x_1)$ | $Max\left\{\frac{q(1+\lambda)(1-\gamma\delta)}{2}(b + a-2x_1),\ 0\right\}$ |
| $x_1 \ge a,$ $x_1 + G \le b$ | $\frac{q\delta\gamma}{b-a}.\begin{pmatrix}(W-a-P).Ln(W-a-P)-\\(W-b-P).Ln(W-x_1-P-G)-(x_1+G-a)\end{pmatrix}+$ $\frac{q\delta(1-\gamma)}{b-a}.\begin{pmatrix}(W-a-P-G).Ln(W-a-P-G)-\\(W-b-P-G).Ln(W-x_1-P-G)-(x_1-a)\end{pmatrix}+$ $\frac{q(1-\delta)}{b-a}.\begin{pmatrix}(W-a-P).Ln(W-a-P)-\\(W-b-P).Ln(W-x_1-P)-(x_1-a)\end{pmatrix}+$ $(1-q).Ln(W-P)$ | $\frac{q(1+\lambda)}{2(b-a)}(b-x_1)^2$ | $Max\left\{\frac{q(1+\lambda)}{2(b-a)}\left\{(b-x_1)^2-\gamma\delta G^2\right\},\ 0\right\}$ |
| $x_1 \ge a,$ $x_1 + G > b$ | $\frac{q\delta\gamma}{b-a}.\begin{pmatrix}(W-a-P).Ln(W-a-P)-\\(W-b-P).Ln(W-b-P)-(b-a)\end{pmatrix}+$ $\frac{q\delta(1-\gamma)}{b-a}.\begin{pmatrix}(W-a-P-G).Ln(W-a-P-G)-\\(W-b-P-G).Ln(W-x_1-P-G)-(x_1-a)\end{pmatrix}+$ $\frac{q(1-\delta)}{b-a}.\begin{pmatrix}(W-a-P).Ln(W-a-P)-\\(W-b-P).Ln(W-x_1-P)-(x_1-a)\end{pmatrix}$ $+(1-q).Ln(W-P)$ | $\frac{q(1+\lambda)}{2(b-a)}(b-x_1)^2$ | $Max\left\{\frac{q(1+\lambda)(1-\gamma\delta)}{2(b-a)}(b-x_1)^2,\ 0\right\}$ |

## Appendix Section 4: Claim oriented secondary loss based analysis

*Claim oriented risk perception loss in stakeholders, and under-claiming strategy of the insured firm with deductible and cap provisions in cyber insurance*

Denote $y(x)$ as the claim function. Firms differ in the way they are exposed to post-claim risk perception loss $g(I(y(x)))$. Companies dealing in sensitive personal information, engaged in major e-commerce activities, or with little brick and mortar presence may likely experience high exposure from $g(I(y(x)))$. These firms are also highly exposed to cyber risks because of the nature of their business. Consider $F_d$ to be one such firm and represent its secondary losses by a convex loss $g(I(y(x)))$, such that $g(0)=0$, $g'(I)\geq 0$, $g''(I)>0$. What this means is that as the stakeholders come to know of larger breaches through a realized indemnity, the IT security health perception about $F_d$ is adversely revised at an increasing rate. Also, consider that the loss from cyber risk can assume any value in the positive line and the cyber contract is written with a deductible $x_1$ and a cap $x_2$.

**Proposition 2** *Facing a convex risk perception loss $g(I(y))$, for every realization$x$ of its random cyber loss$\tilde{X}$, an insured firm claims $y=Min\{x,x_2,\xi*\}$, $(\xi*=I^{-1}(g'^{-1}(1)))$, when $Min\{x,x_2,\xi*\}>x_1+g(Min\{x,x_2,\xi*\}-x_1)$; else the firm does not claim.*

*Proof* Let the net revenue from indemnity be $R(y)=I(y)-g(I(y))$; From F.O.C., $g'(I(y))=1$ is the condition for optimal claim because the second order derivative $R''(y)=I''(y)\{1-g'(I(y))\}-I'(y)^2g''(I(y))$ is clearly negative at $g'(I(y*))=1$.

Denote $\xi*=I^{-1}(g'^{-1}(1))$, and consider the following cases:

**Case-1:** $x\leq x_1$**.**

Because $y\leq x$, and$x\leq x_1$, $I(y)=0$, $g(I(y))=0$, $R(y)=0$, insured firm does not claim.

**Case-2:** $x_1<x$**.**

**Sub case 2A**: $\xi*>x$.

Knowing $g(0)=0$, $g'(I(\xi*))=1$ and $\xi*>x$, $1-g'(I(y))$ is positive in the range$x_1<x<\xi*$**.** Thus $R'(y)=I'(y)\{1-g'(I(y))\}$ is positive when$I'(y)>0$, ($I'(y)>0$ in the range $x_1<y\leq x_2$) and 0 when $I'(y)=0$ (true in the range $x_2<y$). Beginning at $x_1$, the value of $I(y)$ increases monotonically till $y=x_2$, beyond which it remains constant. However, if $x<x_2$, the firm may claim only up to $y=x$. In other words, the firm claims Min$\{x, x_2\}$. $R=Min\{x,x_2\}-x_1-g(Min\{x,x_2\}-x_1)$, and the firm claims when $R>0$. Thus the effective claim strategy is: $Claim\ Min\{x,x_2\}$, $only\ when\ Min\{x,x_2\}>x_1+g(Min\{x,x_2\}-x_1)$; *else do not claim.*

**Sub case 2B**: $\xi*\leq x$.

Here $F_d$ claims $Min\{\xi*,x_2\}$ when $Min\{x,x_2\}>x_1+g(Min\{x,x_2\}-x_1)$.

This defines an effective under-claiming range $x-\xi*$ when $\xi*<x$. *Q.E.D.*

## References


2008 Annual Study: Cost of a Date Breach - Understanding Financial Impact, Customer Turnover and Preventive Solutions. Ponemon Institute, LLC.

Anderson, R., & Moore, T. (2007). *The economics of information security: A survey and open questions. Proceedings of the Fourth biannual Conference on the Economics of the Software and Internet Industries*. France: Toulouse.

Arrow, K. J. (1971). *Essays in the theory of risk bearing*. Chicago, IL: Markham Publishing Co.

Baer, W. S. (2004). Private sector incentives for managing security. In E. O. Goldman (Ed.), *National Security in the information age*. Routledge.

Baer, W. S., & Parkinson, A. (2007). Cyber insurance in IT security management. *IEEE Security and Privacy, 5*(3), 50–56.

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.

Berinato, S. 2008. Data Breach Notification Laws, State By State. Available at http://www.csoonline.com/article/2122493/compliance/cso-disclosure-series—data-breach-notification-laws–state-bystate.html.

Bohme, R. (2005). *Cyber insurance revisited*. Boston, USA: Proceedings of the Workshop on the Economics of Information Security.

Bohme, R., & Kataria, G. (2006). *Models and measures for correlation in cyber insurance*. Boston USA: Proceedings of the Workshop on the Economics of Information Security.

Bohme, R., & Schwartz, G. (2010). *Modeling cyber-insurance: Towards a unifying framework*. Cambridge USA: *Proceedings of the Workshop on the Economics of Information Security.*

Borch, K. (1960). The safety loading of reinsurance premiums. *Skandinavisk Aktuarietidtidskrift, 43*, 163–184.

Bowers, N. L., Gerber, H. U., Hickman, J. C., Jones, D. A., & Nesbit, C. J. (1997). *Actuarial mathematics* (2nd ed.). Schaumburg, IL: Society of Actuaries.

Calandro, J., Matrejek, E., Pollard, N. (2014). Managing cyber risks with insurance: Key factors to consider when evaluating how cyber insurance can enhance your security program. Price Water House Publication number BS-14-0534-A.0614. Available at (http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-managing-cyber-risks-with-insurance.pdf).

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *The Journal of Computer Security, 11*(3), 431–448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcement on market value: capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70–104.

Ernesto, V. d. S. (2009). Mininova Hit By Massive DDoS Attack. Available at https://torrentfreak.com/mininova-hit-bymassive-ddos-attack-090307/.

Evers, J. (2007). T.J. Maxx hack exposes consumer data. C-Net news, available at https://www.cnet.com/news/t-j-maxxhack-exposes-consumer-data/.

Fang, F., Parameswaran, M., Zhao, X., & Whinston, A. B. (2014). An economic mechanism to manage operational security risks for inter-organizational information systems. *Information Systems Frontiers, 16*(3), 399–416.

Floresca, L. 2014. Cyber Insurance 101: The basics of cyber coverage. Available at https://wsandco.com/cyber-liability/cyber-basics/.

Fourth Annual US Cost of Data Breach Study. (2008). Ponemon Institute LLC.

Global Cyber Impact Report. (2015). Ponemon LLC. Available at (http://www.aon.com/attachments/riskservices/2015-Global-Cyber-Impact-Report-Final.pdf).

Global Information Security Survey. (2008). Ernst and Young LCC. Available at (http://www.ey.com/Global/assets.nsf/UK/Global_Information_Security_Survey_2008/$file/EY_Global_Information_Security_Survey_2008.pdf).

Gollier, C. (1996). Optimal insurance of approximate losses. *The Journal of Risk and Insurance, 63*(3), 369–380.

Gollier, C., & Pratt, J. W. (1996). Risk vulnerability and the tempering effect of background risk. *Econometrica, 64*(5), 1109–1123.

Gordon, L. A., Loeb, P. M., & Sohail, T. (2003). A framework for using insurance for cyber risk management. *Communications of the ACM, 46*(3), 81–85.

Hartwig, R. P., & Wilkinson, C. (2014). *Cyber risks, the growing threat*. USA: Insurance Information Institute.

Johnson, T. A. (2014). *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*. USA: CRC Press.

Kovacs, P., Markham, M., Sweeting, R. (2004). Cyber incident risk in Canada and the role of cyber insurance. Institute for Catastrophic Loss Reduction. ICLR Research Paper Series - No. 38.

Mader, B. 2002. Cyber insurance's higher rates make it a long-term sell. (Available at http://sanjose.bizjournals.com/sanjose/stories/2002/11/04/focus2.html).

Majuca, R. P., Yurcik, W., Kesan, J. P. (2006). The Evolution of cyber insurance. (Available at http://arxiv.org/ftp/cs/papers/0601/0601020.pdf).

McLeod, D. 2015. Increased cyber losses means more litigation over claim. Business Insurance. (Available at http://www.businessinsurance.com/article/20150222/NEWS06/303019999/1248).

Meland, P. H., Inger, A. T., & Solhaug, B. (2015). Mitigating risk with cyber insurance. *IEEE Security and Privacy, 6*, 38–43.

Moore, T. (2005). *Countering hidden-action attacks on networked systems. Proceedings of the Workshop on the Economics of Information Security*. Cambridge: USA.

Mossin, J., & Smith, T. (1968). Aspects of rational insurance purchasing. *Journal of Political Economy, 76*, 533–568.

Nelson, S. D., Simek J. W. 2005. Cyber insurance: singing in the Rain. (Available at http://www.senseient.com/pdf/CYBER *INSURANCE.pdf*).

Ogut, H., Raghunathan, S., & Menon, N. (2005). *Cyber insurance and IT security investment: Impact of interdependent risk*. Cambridge, USA: Proceedings of the Workshop on the Economics of Information Security.

Pols, J., Parker, D. 2008. The great debate: security spending. Information Systems Security Association Journal, 6(4) ,21-25.

Raviv, A. (1979). The design of an optimal insurance policy. *American Economic Review, 69*, 84–96.

Schlesinger, H. (1981). The optimal level of deductibility in insurance contracts. *The Journal of Risk and Insurance, 48*(3), 465–481.

Schroeder, D. 2014. Cyber Insurance: just one component of risk management. The Walstreet Journal, May 27 2014. Available at http://blogs.wsj.com/cio/2014/03/27/cyber-insurance-just-one-component-of-risk-management/.

Schwartz, G., Shetty, N., & Warland, J. (2010). *Cyber-insurance: Missing market driven by user heterogeneity*. Cambridge, USA: *Proceedings of the Workshop on the Economics of Information Security*.

Siegel, C. A., Ty, R. S., & Serritella, P. (2002). Cyber-risk management: technical and insurance controls for enterprise-level security. *Information Systems Security, 11*(4), 33–49.

Steele, C. (2007). Cyber insurance supplements, not replaces data breach security (Available at http://searchsecuritychannel.techtarget.com/news/article/0289142sid97_ gci1262357 00.html).

The Betterley Report: Cyber risk and Privacy Market Survey (2010). (Available at http://betterley.com/samples/CyberRisk10nt.pdf).

The Betterley Report: Cyber risk Market Survey (2008). (Available at http://www.betterley.com).

The Betterley Report: Cyber/Private Insurance Market Survey. (2015) (Available at http://www.betterley.com).

Richardson, R. (2008). The CSI Computer crime and security survey. Available at (https://www.miel.in/pdfs/CSIsurvey2008.pdf).

The CSI/FBI Computer Crime and Security Surveys 2000-2006. (Available at http://www.gocsi.com).

Wood, L. (2007). Can 'cyber insurance' protect you from data breach catastrophe? (Available at http://tinyurl.com/3co9hd).

**Dr. Tridib Bandyopadhyay** is an Associate Professor and the Academic Director of Masters of Science in Information Systems at Coles College of Business in Kennesaw State University. He is also a continuing Faculty Research Associate of The KSU Center for Information Security Education. He earned his PhD in MIS from The University of Texas at Dallas. He teaches grad courses in Information Security, Emerging Technologies and Innovations in the MBA and MSIS programs. Dr. Bandyopadhyay's research interests include Information Security and Assurance, Cyber Insurance, Cyber Terrorism, and ICT in Development including health issues. Dr. Bandy welcomes collaborative research, and has worked with professors and students from universities in US and Africa. His research works have been published in peer reviewed journals like ISF, CACM, ITM, IJICTE, and also in the proceedings of national and international conferences.

**Vijay Mookerjee** a Ph.D. in Management, with a major in MIS, from Purdue University. His current research interests include social networks, optimal software development methodologies, storage and cache management, content delivery systems, and the economic design of expert systems and machine learning systems. He has published in and has articles forthcoming in several archival Information Systems, Computer Science, and Operations Research journals. He serves (or has served on) on the editorial board of Management Science, Information Systems research, INFORMS Journal on Computing, Operations Research, Decision Support Systems, Information Technology and Management, and Journal of Database Management.