Is an Ounce of Prevention Worth a Pound of Cure? Balancing Ex Ante Security with Ex Post Mitigation

Veronica Marotta), Heinz College, Carnegie Mellon University
Sasha Romanosky) RAND Corporation
Richard Sharp), Starbucks
Alessandro Acquisti ( ), Heinz College, Carnegie Mellon University

Abstract

Information security controls can help reduce the probability of a breach, but cannot guarantee that one will not occur. In order to reduce the costs of data breaches, firms are faced with competing alternatives. Investments in ex ante security measures can help prevent a breach, but this is costly and may be inefficient; ex post mitigation efforts can help reduce losses following a breach, but would not prevent it from occurring in the first place. We apply the economic analysis of tort and accident law to develop a two-period model that analyzes the interaction between a firm and its consumers. The firm strategically chooses the optimal amount of ex ante security investments and ex post mitigation investments in the case of a breach; consumers, that can engage in ex post mitigation activities. We show that it can be optimal for a firm to invest more in ex post mitigation than in ex ante security protection. However, there also exist situations under which a firm finds it optimal to *not* invest in ex post mitigation, and simply invest a positive amount ex ante. In addition, we find that a social planner seeking to minimize the social cost from a breach should not incentivize the firm to bear all consumers loss: as long as consumers have feasible tools for mitigating the downstream impact of data breaches, they should be responsible for a fraction of the expected loss caused by the breach.

Keywords*: Information security, data breach disclosure, economic analysis of tort law, identity theft, analytical modeling, ex ante prevention, ex post mitigation*

1. INTRODUCTION

Data breaches, like many kinds of accidents, are inevitable. Firms face several options when considering how to invest in securing their information systems from cyber-attack or improper use. The worldwide market for corporate information security products reached over $60 billion dollars in 2013 (Gartner, 2013) and the US Government alone spent approximately $65 billion on security controls between 2006 and 2013 (Coburn, 2014). However, even with those security investments, accidents remain inescapable: “Even a well-defended organization will inevitably experience a cyber incidence at some point” (Justice, 2013). Citing more than 800 million records lost in 2013, one research firm concluded that we have reached a point where “breach[es] and data theft are inevitable” (ABI, 2014). Another study found that 56% of firms had experienced one or more material security incidents within the past 2 years, with an average cost of $5.4 million per data breach (Ponemon 30.61). For instance, TJMax suffered costs over $250 million due to a breach in 2007 (TJX, 2007), Heartland Payment Systems spent $150 million in legal fees and fines from its breach of 100 million credit cards in 2007 (Yadron, 2014), and Target reported $235

million in expenses from its 2013 data breach. The cost of the recent Experian breach are still not known, but they may end up being significant.

As a result of those breaches and the costs they cause to both firms and consumers, most U.S. states have enacted data breach disclosure laws that require organizations to notify individuals when personally identifiable information has been lost or stolen (Marushat, 2009). By forcing firms to notify consumers of a breach, the argument goes, firms will be incentivized to invest in sufficient security controls to prevent them (Majoras, 2005). A further consequence of the publicity from disclosure is that firms bear will additional costs due to notification, customer support operations, litigation, customer churn, and loss of reputation (Gao 2007; Ponemon, 2011). The strategic decision for the firm, therefore, is understanding the balance between ex ante security investments (i.e. those that serve to prevent a breach from occurring in the first place), and ex post mitigating investments (i.e. those that help reduce disclosure costs and any reputation harms). On one hand, investing in prevention measures is costly, but avoids potentially catastrophic losses in case of a breach. On the other hand, if breaches are rare and relatively low in magnitude, it may be cheaper to focus on mitigating the cost ex post, without investing (excessively) in prevention measures. This trade-off was exemplified in a 2005 analysis by Gartner, which estimated that every $1 spent preventing a breach saves almost $6 in mitigation costs (Yadron, 2014). And yet, firms respond with claims that "it costs more to secure the system than to suffer the breach" (Yadron, 2014). Further, one security research firm found that investments in incident response activities (i.e. ex post measures) were more appropriate than prevention controls, such as vulnerability scans and user awareness (Westervelt, 2014).

The dilemma faced by firms is a traditional problem of intertemporal allocation of resources under uncertainty. However, firms' security investments are not borne in isolation. Consumer losses and, therefore, consumer behavior, are both affected by a firm's actions. In many cases, consumers bear substantial harm following financial or medical identity theft associated with data breaches. For example, there were approximately 16.6 million household victims of identity theft in 2012 (in part attributable to data breaches), with total (direct and indirect) losses of $24.7 billion (Harrell, 2014). In this manuscript, we leverage insights from the economics of accident law to model the interaction between firm and consumers, with the first facing the threat of a breach, and the latter facing the threat of identity theft.

Policy makers have a key incentive to drive policy interventions that minimize aggregate costs. For example, following the direction of a Presidential Executive order to protect critical infrastructure, NIST created a collection of recommendations for protecting digital assets (NIST, 2014). In this paper, we apply the economic analysis of tort and accident law to an information technology problem and we propose a novel framework that allows us to investigate the strategic interaction between a firm that invests in security and its consumers. We build a two-player, two-period model where the firm needs to balance ex ante investments in security protection (in the first period) with ex post investments in mitigation activities in the case a breach occurs (in the second period). Additionally, consumers themselves can act in the second period to attempt to mitigate their expected loss in the case of a security breach. Additionally, our framework allows us to analyze the conditions under which a social planner can minimize aggregate costs by setting the proportion of consumer expected loss that should be borne by the firm.

We solve model through the definition of specific functional forms and find that, under various conditions, a firm would optimally invest more in ex post mitigation, after the breach has happened, than in ex ante prevention. However, there also exist situations under which a firm may find it optimal to *not* invest in ex post mitigation and invest a positive amount in ex

ante prevention. In addition, we find that a social planner seeking to minimize the social cost from a breach should not incentivize the firm to bear all consumers loss. In fact, the maximization of social welfare (that, in this specific case becomes minimization of aggregate costs) requires consumers to always bear some fraction of their expected loss from a security breach.

The paper proceeds as follow: section 2 reviews existing works in information security and information systems; in section 3, we setup the model and describe the game between the firm and consumers. Section 4 presents the general analysis of the two players' behavior while section 5 exemplifies the model for the case of specific functional forms and presents the results from numerical simulation of the model; section 6 presents the social planner problem and how it can intervene to maximize social welfare. Finally, section 7 concludes.

2. BACKGROUND

The body of IS literature related to information security has grown considerably in recent years. Significant attention in this field has been paid to optimal investment in security (Lui, 2011; Laube, 2015; Lee, 2011; Cezar, 2014) and the disclosure of breaches, vulnerabilities, and software bugs (Cavusoglu, 2008; Telang and Wattal, 2007; Gandal et al., 2009; Grossklags et al., 2008). Scholars have empirically investigated the effect of disclosing data breaches on stock market valuation (Campbell et al., 2003; Cavusoglu et al.,2004; Acquisti et al., 2006; Kannan et al., 2007) and consumer identity theft (Romanosky, 2011), as well as the effect of disclosure of security-related activities in financial statements Gordon et al., 2006; Wang et al., 2009). Empirical research has also investigated the effect of disclosure polices on health outcomes (Jin and Leslie, 2003), financial securities (Barth and Cordes, 1980), and US policy making generally (Fung et al., 2007). Accounting research has also developed theories explaining shareholder investment and a firm's financial disclosure decisions (Verrecchia, 2001). Most related to this paper is theoretical work by Gordon and Loeb (2002), who examine the optimal investment in security measures and, as an optimization problem, conclude that a firm should not (necessarily) address the most severe vulnerabilities first, but focus on those improvements for which the marginal gain is greatest. Gordon and Loeb find that investments should be less than one-third of the expected loss from a breach. This work, however, examines ex ante security measures only, and not ex post mitigation efforts.

From a modeling perspective, we leverage the economics of tort law (Shavell, 1984), Kolstad et al., 1990; Landes and Posner, 1987). This body of work examines the impact of alternative policy regimes (often in the context of liability rules) on injurer and victim behaviors. For example, consider an individual driving a car on a roadway. The driver engages in some level of care (prevention) to avoid an accident, and assumes some probability of an accident occurring. A rational driver seeks to minimize her private costs by balancing the cost of care, plus the expected damage from an accident. However, this behavior will be suboptimal whenever the driver does not bear the full costs of her actions (for instance, the costs inflicted on pedestrians). The objective of the social planner, therefore, is to devise a policy that induces drivers (and pedestrians) to take the socially optimal level of care, thereby minimizing aggregate costs incurred by all parties. We therefore leverage this modeling approach to analyze firm and consumer behavior in the context of data breaches.

Despite the prevalence of security technologies available to firms, data breaches still occur and are costly. The trade-off firms face, therefore, is understanding how to balance ex ante prevention investments with ex post mitigation efforts. Resolving this tension has been

especially difficult given the flurry of state legislative efforts in requiring the disclosure of data breaches to affected individuals, which has enabled consumers to both take action to prevent identity theft, while at the same time forcing firms to internalize some of that loss through litigation. Some of the theoretical IS literature has examined optimal investment in security patching and software vulnerability (Arora, 2006; Arora 2010a; Arora 2010b; Arora and Xu, 2007; Cavusoglu, 2008). However, no analytical research has yet examined the costs and consequences of data breaches regarding ex ante prevention, and ex post mitigation activities, which is our focus.

Our approach differs from traditional IS models involving externalities in various ways. First, we make no assumptions regarding any legal duty by firms to protect consumer data for the simple reason that no uniform standard of care has been established through US statute or common law. This realization allows us to model consumer liability as a continuous (not discrete) variable driven by market and regulatory forces, thereby more realistically reflecting the emerging world of consumer data protection, and the degree to which firms internalize consumer costs. Second, most analyses recognize both the cost of care and expected loss by the injurer (e.g. the firm), but often ignore the cost of care by the victim (e.g. the consumer). We extend traditional accident models by explicitly incorporating the consumer's cost of mitigating actions. Third, we extend previous IS models to specifically account for both ex ante and ex post firm effort. Finally, we proceed beyond typical modeling procedures which directly account for firm or consumer activity, and model aggregate (social) costs at consumer and firm equilibrium levels. That is, we evaluate social cost functions *at agents' privately optimal levels of care*. Therefore, to our knowledge, this article is the first to theoretically analyze firm, consumer, and aggregate costs of data breaches.

3. MODEL SETUP

Consider a firm that invests in many forms of data protection. Conditional on this ex ante investment, it may suffer a data breach that compromises the personal information of its customers. In many cases, once it learns of the breach, the firm will be required to notify affected individuals.[1] The reasons are threefold. First, 48 US states have already enacted disclosure laws, essentially making disclosure a requirement for all firms in the US. Second, firms may disclose the breach even absent legal requirement out of an abundance of caution, fear of customer repercussions, and to avoid legal action brought by state AGs. Finally, it is often the case that any sizable breach involving information likely to lead to consumer harm would require notification, whether because of the cause of the breach, lack of encrypted data, or types of information compromised.[2]

Once consumers are informed of the breach by the firm, they become empowered to act in order to reduce any identity theft, such as closely monitoring their credit reports or placing a credit freeze on their accounts. But the firm's responsibilities are not over. Once it

[1] Certainly, before a firm can notify individuals it must become aware of the breach. This may occur in several ways. In some cases, the firm is contacted by a third party, such as a payment card processor (as in the case of the Neiman Marcus breach (Kingston 2014)), or law enforcement (as in the case of the Target breach (Mulligan 2014)). Sometimes individuals become aware and notify the company, and certainly, in other cases, the firm, itself, is first to discover the breach (Trustwave 2014). For our analysis, however, the method by which the firm learns of the breach does not drive disclosure, and is therefore not considered.

[2] Conceivably, it may still be the case that despite the many incentives for disclosure, firms will not disclose a breach. First, a firm (and everyone else) may continue forever never having known it was breached. It is also conceivable that firms may learn of a breach, and illegally conceal it. However, conversations with privacy attorneys confirm that firms are keenly aware of the consequences that come with violation of such laws. In addition, some states provide exceptions to disclosure if, for example, the information was encrypted, if the number of records compromised did not exceed the threshold (often 500), or if the types of information compromised are not deemed likely to lead to consumer harm (BakerHostetler 2014). However, given that we model the costs borne by firms that suffer publicly disclosed data breaches, for our analysis, we do not consider undisclosed breaches. Moreover, that a firm has not yet had to disclose a breach does not make it immune from future potential disclosures.

has publicly disclosed the breach, it faces additional costs from regulators, law enforcement, customers and shareholders, who may each impose fines, require forensic investigations, bring class action lawsuits, or affect market valuation. Therefore, the firm is driven to invest in numerous ex post activities in the hopes of minimizing future costs and restoring its reputation.

Below, we formalize the firm, consumer and social cost functions. We assume that both firms and consumers seek to minimize their private costs by optimizing their amount of care. For instance, the firm seeks to minimize costs over both ex ante and ex post effort.[3] The social planner, on the other hand, seeks to minimize overall costs through policy interventions, which we discuss below. We first analyze firm and consumer behavior, and then examine social welfare.

3.1 Firm Costs

The firm's level of ex ante data protection, $x_1 \geq 0$, represents the amount of investment in all forms of security activities designed to prevent a data breach. Such ex ante measures include, among others, network access controls, firewalls, software patching, and employee training. However, these investments come at a cost, $c(x_1)$, which we assume to be increasing and convex in activity, continuous and twice differentiable ($c'(x_1) > 0$, $c''(x_1) > 0$, $c(0) = 0$). We denote the probability that a breach will occur given this level of investment as $p_B(x_1)$, decreasing and convex in x_1, also continuous and twice differentiable ($0 \leq p_B(x_1) \leq 1$, $p_B'(x_1) < 0$, $p_B''(x_1) > 0$, $p_B(0) = 1$).

Once a breach occurs, however, the firm bears numerous costs. First, immediately following the breach, it must determine the cause of the incident, repair any damaged IT systems, and ensure business services are fully operational (Lemos, 2009). We model this fixed cost of investigation as $i > 0$.

In addition, faced with possible reputation harms stemming from the loss of new or existing customers, stock market or brand devaluation, the firm engages in numerous ex post mitigating activities, $x_2 \geq 0$, in order to reduce these reputation effects.[4] For example, it can demonstrate a sense of responsibility and accountability to affected individuals by providing prompt and actionable notification. It can establish customer support centers to assist consumers with any questions. It can engage marketing firms to communicate the steps the firm is taking to re mediate any damage, and it can offer credit monitoring or identity theft insurance to affected individuals.[5] We denote the magnitude of this reputation loss as $r(x_2) \geq 0$ which we assume is decreasing and convex in x_2.[6] Of course, all of these ex post investments come at a cost, and so we denote the cost of these activities as $d(x_2) \geq 0$ which is increasing and convex in x_2, continuous and twice differentiable.

---

[3] Note that throughout this manuscript, the terms ex ante/ex post and prevention/mitigation are used interchangeably. We also use the terms care, controls, measures, and investments interchangeably to refer to activities taken by the firm to either prevent a breach or reduce the cost from a breach.

[4] See also (Homan and Shih 2014) and (Hogan and Lovells 2014) describing mitigation efforts generally, and Ponemon (2013) describing a US customer churn rate of about 3% following a breach. Target also suffered a net $17m loss from its recent breach due to investigating the data breach, offering credit-monitoring and identity-theft protection services to customers, increased staffing in call centers, and legal expenses and a profit loss of almost 50% in Q4, 2013 (McGrath 2014).

[5] Choicepoint paid $5 million in consumer redress (Brodkin 2007), the Veterans Aairs agency agreed to pay $20 million in consumer redress, including credit card monitoring in response to a breach (Pulliam 2007).

[6] That is, the more effort the firm takes in improving reputation, the less of an economic impact the firm will suffer.

The final cost borne by the firm stems from 3rd party litigation. When consumers are sufficiently angered by the alleged bad practices of the firm, they may bring legal actions to recover any losses (Romanosky, 2014). For example, the Heartland breach involving 130 million records resulted in settlements totaling more than $100 million (Kaplan, 2010). Note that while consumers may seek compensation for all costs they are generally only compensated for a portion of actual financial loss (described further below). Therefore, we indicate the fraction of consumer harm internalized by the firm as αH_{ID}, where H_{ID} is the expected loss from identity theft, and $0 \leq \alpha \leq 1$. A value of $\alpha = 1$ implies that the firm internalizes all consumer harm, while a value of $\alpha = 0$ implies that the firm bears no consumer harm. Because some ex post firm actions may also help reduce the amount of consumer fraud (such as timely notification, cancelling transactions, or replacement of payment cards), we represent this final cost borne by the firm as $\alpha H_{ID}(x_2, y)$.[7]

3.2 Consumer costs

We have noted how notification of a breach enables consumers to react and reduce expected losses from identity theft. For example, after being notified of the theft of one's financial documents, an individual can closely monitor her credit report, place a credit freeze or fraud alert on her account, sign up for identity theft insurance or credit monitoring, and close any fraudulent accounts. We denote this level of activity as $y \geq 0$.

An important consideration is that consumers bear two distinct types of costs: the financial loss from identity theft, $h_{ID} \geq 0$, and the time and effort exerted to reduce that loss, $h_{TE} \geq 0$. We assume that a consumer's expected losses are decreasing and convex in consumer care. Moreover, for generalizability, we assume that ex post firm actions are also able to mitigate identity theft by reducing expected losses. i.e. $H_{ID}(x_2, y) = p_{ID}(x_2, y)*h_{ID}(x_2, y)$, where $0 \leq p_{ID}(x_2, y) \leq 1$.[8] For brevity, however, we do not distinguish between the probability of identity theft and the magnitude of harm; we simply refer to the expected harm throughout the remainder of this document. Recall from above that only a portion of an individual's actual financial loss is typically compensable under state laws, while time and effort is generally not (Wolf, 2011). Therefore, we denote the portion of expected financial loss borne by consumers as $(1 - \alpha)H_{ID}(x_2, y)$.

Finally, we assume that the cost of time and effort, $h_{TE}(y)$, in reducing identity theft is increasing and convex in y.

3.3 Sequence of Events

The sequence of events is shown in Figure 1 where we illustrate a two-player, combined sequential and simultaneous two-period game.

[7] For example, swift response by Target was initiated to help assuage consumers and the threat of litigation (Orrick 2014), and a class action suit against a county community college was brought, in part, because of delayed notification on the part of the college officials (Robinson 2014).

[8] Not all breaches result in identity theft. For example, a firm may carelessly dispose of financial records in a dumpster (the data breach), but those records may never be used to commit fraud. Therefore, even absent ex post firm or consumer action, identity theft would still not occur. We can account for this by including an additional parameter, 0 < p0 <1 to our model. However, given that, by definition, it is independent of firm or consumer action, it would not qualitatively affect our results. Thus, we omit it for brevity.

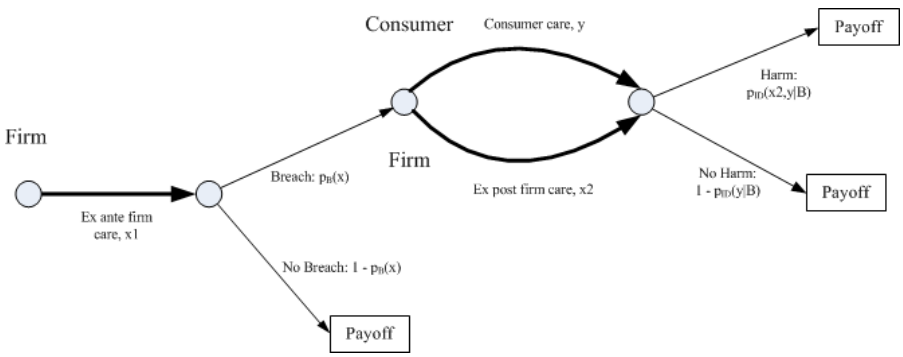

Figure 1: Sequence of events

In the first period the firm determines its optimal level of ex ante breach prevention, x_1, after which a breach will occur with probability $p_B(x_1)$. In the second period, the firm and consumer simultaneously choose their levels of activity that each minimize their total costs. The firm engages in ex post activities to minimize breach costs and the impact to its reputation, while the consumer engages in activities to minimize her losses from identity theft. Finally, a consumer will suffer identity theft with probability $p_{ID}(x_2, y|B)$, and harm $h_{ID}(x_2, y)$.[9]

The firm's objective is to determine the level of ex ante (x_1) and ex post (x_2) effort that minimizes its total costs:

$$F(x_1, x_2, y) = c(x_1) + p_B(x_1)(i + d(x_2) + r(x_2) + \alpha\, H_{ID}(x_2, y)) \qquad \text{Eq. 1}$$

The consumer chooses a level of care, y, that minimizes her total costs:

$$C(x_2, y) = p_B(x_1)(h_{TE}(y) + (1 - \alpha)\, H_{ID}(x_2, y)) \qquad \text{Eq. 2}$$

The aggregate (social) cost is the sum of the firm and consumer cost functions:

$$S(x_1, x_2, y) = c(x_1) + p_B(x_1)(i + d(x_2) + r(x_2) + H_{ID}(x_2, y) + h_{TE}(y)) \qquad \text{Eq. 3}$$

4. ANALYSIS

4.1 Equilibrium solutions

We find the solution (or solutions) to the model by backward induction. We define $\tilde{x}_1$, $\tilde{x}_2$, respectively, as the levels of ex ante and ex post firm care that minimize its private costs; $\tilde{y}$, as the level of care that minimizes the consumer's private costs; and x_1^*, x_2^* and y^*, respectively, as the levels of firm and consumer care that minimize overall aggregate costs.

First, we solve the two-player simultaneous game in which the firm and consumer determine the values of x_2 and y (Eq. 1, and Eq. 2). Note that x_1 drops out of these equations, demonstrating how the equilibrium values of x_2 and y are independent of x_1. Of course, firm and consumer *costs* at the equilibrium quite explicitly depend on x_1. Once the equilibrium values of x_2 and y are known (and due to the independence just noted, we now know these as values, not just expressions in terms of x_1), we obtain a convex optimization problem in x_1 defined by the derivative of Eq. 1 with respect to x_1 set equal to zero.[10]

[9] We model a data breach and the fraudulent use of consumer data as distinct and sequential events. For example, a firm may carelessly dispose of financial records in a dumpster (the data breach), but those records may or may not be used to commit subsequent identity theft.

[10] In some cases, it may be difficult to solve the (x2; y) system algebraically, however, one may apply a numerical method based on fixed point iteration that quickly converges to the solution in practice.

In this game, the existence of an equilibrium follows from the observation that the scenario is a continuous, two-player game with bounded strategy sets. Consumer and firm activity are non-negative and, for practical purposes, finite. As such, a general solution to the two-player continuous game exists (Glicksberg, 1952). Additionally, if the game is diagonally strictly convex, then the solution is also unique (Glicksberg, 1952).

Both proofs are based on Glicksberg's theorem (Ozdaglar, 2010, slide 4). In the Appendix, we provide detailed proofs for this and other propositions.

Next we describe the characteristics of the general solution concerning firm and consumer behavior.

4.2 Firm and consumer behavior

Because we are interested in firm costs and behavior before and after data breach, we examine how the firm's decisions and outcomes (i.e. its costs, and ex ante, and ex post activities) are driven by the components of Eq. 1.

Note, from Eq. 1, that absent the public disclosure of a breach,[11] the firm would incur no ex post costs, either from reputation, disclosure or consumer redress, but only the direct cost of breach investigation, i. It would therefore seek to minimize only ex ante costs, x_1. However, the public disclosure of a data breach drives the firm to optimize its behavior in two ways as shown in Figure 2. First, it seeks to minimize ex post mitigation costs (left panel) which include the cost of breach investigation, i, the increasing cost of disclosure, $d(x_2)$, the decreasing costs of reputation and consumer redress, $r(x_2)$ and $\alpha H_{ID}(x_2, y)$. Next, it seeks to minimize ex ante prevention costs (right panel) which consist of the increasing cost of prevention controls, $c(x_1)$, and the decreasing expected losses from the breach, $p_B(x_1)(.)$.

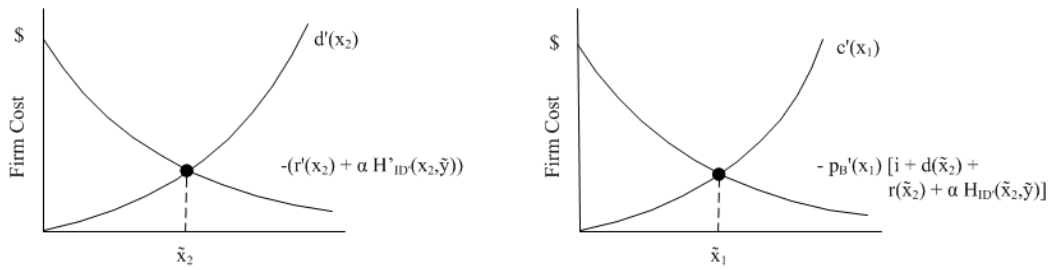

Figure 2: Two optimization problems

In addition, observe that an increase in ex post breach costs (disclosure, reputation, or consumer redress) will increase expected losses from a data breach and drive up prevention efforts, illustrating how ex ante prevention is affected by ex post losses (i.e. breach *prevention* is driven by breach *mitigation*). However, the opposite is not true (i.e. mitigation is not affected by prevention). The amount of mitigation effort spent trying to reduce the impact from a data breach is not a function of any efforts spent trying to prevent that breach from occurring. Once the breach has occurred, the firm's focus now turns to minimizing ex post costs – whatever was (or was not) spent becomes immaterial.

Efforts taken by firms to reduce the effects of a data breach are affected by several factors. First, as the cost of responding to breaches and notifying consumers decreases, $d(x_2)$, the overall effort taken to reduce ex post costs will increase because the benefit enjoyed from

[11] Again, we make no comment as to the reason for disclosure, only simply the disclosure itself, and subsequent costs.

spending more has risen. This might occur, for example, if cheaper ways were found of notifying individuals, or if the firm's cost of providing credit monitoring or identity theft insurance decreased. While these cheaper costs of disclosure would increase mitigation *efforts*, they would reduce total breach *costs*.

Note that neither the firm nor the consumer bear the full cost of their actions, and neither will engage in the socially optimal level of care.

PROPOSITION 1. *As the cost of disclosure decreases, firms will increase their level of ex post effort in order to mitigate the consequences of a breach. If* $\tilde{d}(x_2) = ad(x_2) + b < d(x_2)$ *for all* x_2*, where a and b are constants, then* $\tilde{x}_2 > x_2$ *given y.*

Complete proof is in the Appendix.

Conversely, the firm will decrease its ex post activity if either the reputation loss, $r(x_2)$, or amount of internalized consumer harm, $\alpha H_{ID}(x_2, y)$, decreases. This is because the relative benefit of trying to mitigate expenses is lower. For example, as consumers become desensitized to yet another revelation about a data breach, or as shareholders begin to consider breaches as simply the cost of doing business. The firm would also reduce mitigation efforts either when its liability, α, or the overall amount of consumer identity theft decreased. Liability could decline as judicial rulings dismiss more data breach lawsuits, or as settlement awards dry up.[12] And consumer identity theft would decline as consumers, themselves, begin to take more action to reduce their losses.

PROPOSITION 2. *As reputation costs decrease, firms will decrease their level of ex post mitigation effort. If* $\tilde{r}(x_2) = ar(x_2) < r(x_2)$ *for all* x_2 *where* $0 < a < 1$*, then* $\tilde{x}_2^* < x_2^*$ *given y.*

Complete proof is in the Appendix.

Next, the amount of security investment taken ex ante, x_1, is affected by several important factors. First is the market cost of security (prevention) controls. When the cost of breach prevention technology decreases, the marginal benefits enjoyed from them increases, driving up the level of investment.

PROPOSITION 3. *As breach prevention technologies become cheaper, firms will invest more and enjoy lower total costs. If* $\tilde{c}(x_1) = ac(x_1) + b < c(x_1)$ *for all* x_1 *where a and b are constants, then* $\tilde{x}_1 > x_1$ *and* $F(\tilde{x}_1, x_2, y) < F(x_1, x_2, y)$*.*

Complete proof is in the Appendix.

However, as the effectiveness of these controls improves (i.e. as they become better at stopping or neutralizing cyber-attacks), the probability of any successful attack decreases for any given level of investment. This in turn reduces the optimal amount of prevention in which a firm needs to invest in order to minimize its costs.

PROPOSITION 4. *As security technologies becomes more efficient in preventing breaches, firms will spend less on them, lowering their total overall costs. If* $\tilde{P_b}(x_1) = aP_b(x_1) + b < P_b(x_1)$ *for all* x_1 *where a and b are constants, then* $\tilde{x}_1 < x_1$ *and* $F(\tilde{x}_1, x_2, y) < F(x_1, x_2, y)$*.*

Complete proof is in the Appendix.

The decrease in effort is shown in the same manner as the decrease in effort in Proposition 2, and the lower overall costs are shown in the same manner as in Proposition 3.

[12] Research, in fact, shows a declining breach litigation rate with current estimates around 3-4% (Romanosky 2014).

4.3 Consumer behavior

Similar to firm's behavior, consumer effort is affected by the components of Eq. 2. First, as the cost of engaging in ex post mitigation activities increases, $h_{TE}(y)$, the overall effort taken by consumers ex post, given the firm's effort, will decrease.

PROPOSITION 5. *As the cost of ex post consumer mitigation activities increases, consumers will decrease their level of ex post effort. If* $\tilde{h}_{TE}(y) = ah_{TE}(y) + b > h_{TE}(y)$ *for all* y*, where* a *and* b *are constants, then* $\tilde{y} < y$ *given* x_2*.*

Complete proof is in the Appendix.

Similarly, consumers will decrease ex post effort if the amount of internalized consumer harm, $(1 - \alpha)*H_{ID}(x_2, y)$, decreases. This happens if, for instance, firm's liability increases and therefore consumers must internalized a lower proportion of the expected harm. Similarly, expected loss from identity theft would decrease as firms increase their ex post effort to mitigate the consequences of the breach.

PROPOSITION 6. *As expected loss from identity theft decreases, consumers will decrease their level of ex post mitigation effort. If* $\hat{H}(x_2, y) = aH(x_2, y) < H(x_2, y)$ *for all* y *where* $0 < a < 1$*, then* $\tilde{y} < y$*, given* x_2*.*

Complete proof is in the Appendix.

While these insights are important, they do not yet completely resolve the key research question of this paper - namely, what is the optimal composition of ex ante and ex post investments - which we examine next.

5. MODEL ANALYSIS

5.1 Theoretical Insights

In the previous sections, we have established the conditions for a unique solution to the general model and we have analyzed the behavior of the players in a general setting. In this section, we provide an exemplification of the model by using specific functional forms. Consistent with our initial assumptions of tractable, differentiable forms, we choose linear functions. Some previous models in this space have used fixed parameters, rather than functional forms (Laube, 2013; Lui, 2011; Cavusoglu, 2008). Our using linear functions is in line with other models that employed basic convexity assumptions, for example (Lee, 2011; Cezar, 2014). Additionally, the functions allow us to obtain intuitive results that can be interpreted to gain insights from the model.

We define the cost and probability functions as follows:

$$c(x_1) = \gamma x_1$$

$$p_b(x_1) = (1)/((1 + x_1))$$

$$d(x_2) = \delta x_2$$

$$r(x_2) = (\rho)/((1 + x_2))$$

$$h_T(y) = \eta y$$

$$H(x_2, y) = (\theta)/((1 + x_2)(1 + y))$$

where γ, δ, ρ , η and θ are constants, and are necessarily positive due to the various constraints of the general model. We can write the firm's total cost function as:

$$F(x_1, x_2, y) = \gamma x_1 + (1)/((1 + x_1))[i + \delta x_2 + (\rho)/((1 + x_2)) + \alpha(\theta)/((1 + x_2)(1 + y))]$$

and the consumers' total cost function as:

$$C(x_2, y) = (1)/((1 + x_1))[\eta x_2 + (1 - \alpha)(\theta)/((1 + x_2)(1 + y))]$$

Firms and consumers act simultaneously in the second period. The firm chooses the amount of x_2 that minimizes its cost (given consumers' choice); similarly, consumers choose the amount of y to minimize their cost (given firm's decision). Given the solutions for the privately optimal levels of $x_1$and y, we solve for the firm's first period decision. Lemma 1 presents the equilibrium solutions. Complete derivation is available in the Appendix.

LEMMA 1. *Equilibrium solutions.*

- *Optimal amount of ex post consumers' effort*. In the second period, the privately optimal amount of consumers' effort is equal to: $\tilde{y} = \sqrt{(1-\alpha)\theta/\eta(1+x_2)} - 1$.
- *Optimal amount of ex post firm's investmen*t. In the second period, the privately optimal amount of firm's investment is equal to: $\tilde{x}_2 = \sqrt{\frac{1}{\delta}(p + \frac{\alpha\theta}{(1+y)})} - 1$.

  Optimal amount of ex ante firm's investment. In the first period, the privately optimal amount of firm's investment is equal to: $\tilde{x}_1 = \sqrt{\frac{1}{\gamma}[i - \delta + 2\sqrt{\delta}\sqrt{(p + \frac{\alpha\theta}{(1+\tilde{y})})}} - 1$.

As highlighted before, $\tilde{x_2}$ and $\tilde{y}$ are independent of $\tilde{x_1}$. This reflects in the solutions for the privately optimal levels of firm and consumers' effort illustrated in Lemma 1. The optimal amount of ex ante firm's investment is a function of the second-period parameters, however the reverse is not true. The second period solutions depend on the other player's decision in the same period; intuitively, if the firm increases the level of ex post investment, the optimal amount of consumers' effort decreases, and vice versa. In addition, the optimal amount of consumers' effort increases with the ratio $((1 - \alpha)\theta)/(\eta)$ that captures consumers' cost efficiency: $(1 - \alpha)\theta$ captures the marginal benefit, in terms of reduction in identity theft's cost, of an additional unit of consumers' effort; η captures the marginal cost of an additional unit of consumers' effort.

Similarly, the firm's optimal level of ex post investment decreases with the level of consumers' effort. Furthermore, the firm's optimal level of ex post investment depends on $\rho + \alpha\theta$ and δ. The higher the possible reputation cost or the higher the expected consumers' loss that the firm may have to bear, the higher the incentive of the firm to invest ex post. On the other side, the higher the cost of ex post investment - that is, the higher δ, the lower the incentive of the firm to invest in the second period.

The analysis of the equilibrium solutions reveals an interesting behavior: the firm and consumers may not always find it optimal to invest a positive amount of care. That is, there may be situations where for one of the players it is not optimal to invest, and the burden falls entirely on the other player. Lemma 2 below summarizes the conditions under which such equilibria occur. Complete proof is in the Appendix.

LEMMA 2. *Conditions under which it is optimal to not invest a positive amount.*

- *In equilibrium, the firm does not invest ex post*: when $\sqrt{\frac{(1-\alpha)\theta}{\eta}} \geq \frac{\alpha\theta}{\delta-\rho}$: $\tilde{x_2} = 0$ and $\tilde{y} \geq 0$.
- *In equilibrium, consumers do not invest ex post*: when $\sqrt{\frac{1}{\delta}(p + \alpha\theta)} \geq \frac{(1-\alpha)\theta}{\eta}$: $\tilde{x_2} \geq 0$ and $\tilde{y} = 0$.

The first condition suggests that when the ratio between consumers' proportion of expected loss and marginal cost of ex post investment is greater (or equal) to the ratio between firm's proportion of expected consumers' loss and the difference between marginal cost of ex post investment and reputation cost, it is optimal for the firm to not invest in equilibrium and leave consumers to mitigate the ex post damage. Even if theoretically possible, this equilibrium seems unlikely to happen, as it would require consumers to be efficient enough and to act timely so to also cover for the firm. In reality, consumers may not have the chance to take any action. We explore further these situations using simulations in section 6.

The second condition suggests that when the ratio between the firm's proportion of expected loss, summed with the reputation cost, and the marginal cost of ex post investment is greater (or equal) to the ratio between consumers' proportion of expected loss and marginal cost of ex post investment, it is optimal for consumers to not invest. This situation is more likely to happen as it requires the firm's cost parameters to be greater than consumers' cost parameters. In this case, the firm has an incentive to act promptly and efficiently in the attempt to mitigate ex post loss.

Finally, in the equilibria where the firm finds it optimal to invest both ex ante and ex post, it is interesting to understand whether there would be situations where the firm would find it optimal to invest less ex ante rather than ex post. In reality, firms may have the tendency to over-invest ex ante in the attempt to avoid a breach to happening altogether. Indeed, they may genuinely feel that an ounce of security prevention is worth a pound of cure.

However, this may not be economically optimal, specifically in situations where ex ante costs are prohibitive and it would be cheaper to mitigate ex post costs after a breach. Lemma 3, below, summarizes the condition under which the firm's optimal level of ex ante investment is lower than the optimal level of ex post investment. Complete proof is in the Appendix.

LEMMA 3. *When* $\sqrt{\delta}\frac{(i-\delta)}{(\gamma-2\delta)} < \sqrt{\rho + \frac{\alpha\theta}{(1+\tilde{y})}}$ *the firm's optimal level of ex ante investment is lower than the optimal level of ex post investment.*

Intuitively, when the ex ante marginal investment cost (γ) is high and the ex post marginal investment cost (δ) is low, the first term in the condition tends to be low and the firm finds it convenient to reduce the ex ante investment relative to ex post investment. Similarly, when consumers have not incentive to invest ex post, so that y = 0, the term on the right hand-side tend to increase relative to the term on the left hand-side, pushing the firm to invest a higher amount ex post.

5.2 Simulation Analysis

We investigate the implications of our theoretical results using simulation analysis. Informed by empirical observations, we vary two key consumer parameters, while holding the rest constant. Then, we individually vary firm-specific parameters and examine how the simulation results change.

The consequences to consumers from a data breach can vary considerably depending on the type of information compromised. Reasonably, we can assume that a consumer's expected loss from a breach of highly sensitive information (such as financial history or health information) is higher than that of one involving less sensitive information (such as e-mail addresses, browsing activity, or a password to a non-sensitive account). Therefore, we

vary the parameter θ (the expected consumer loss) which captures the variation of information sensitivity (i.e. high (low) sensitivity translates to high (low) expected loss).

Second, the strategic interaction between the firm and its consumers in the ex post period is fundamental in the determination of the equilibrium outcome. Nevertheless, in practice, there may situations where it is very hard for consumers to act in order to mitigate their losses. For example, in the event of a breach involving health data or biometric information, it is unclear what actions a consumer could feasibly take since this information cannot be reset like a password. Further, for some sectors (such as utilities or telecommunications and broadband internet access), there may be no practical alternative for a consumer, and so a breach by the dominant firm affords no meaningful opportunity for a consumer to change carrier. On the other hand, there are instances where consumers *can* take meaningful actions, such as in the compromise of password, or payment card information, where consumers can buy identity theft insurance, promptly request a new credit card, or change their password. These situations can be modelled by a relatively lower marginal cost for the consumer. Therefore, we vary the parameter η to differentiate situations where consumers can take meaningful actions (low η), from those where they cannot (high η).

The combination of low/high sensitivity information, and consumer action/no action creates four possible scenarios of interest as shown in Table 1.

Table 1: Simulated Scenarios

	Low Sensitivity Information (low θ)	**High Sensitivity Information (high θ)**
Consumers can take action (low η)	E-mail addresses, password to non-sensitive accounts	Financial Data, Payment Cards
Consumers cannot take action (high η)	Demographic Information (cannot be changed)	Medical, Biometric, Social Security Numbers (cannot be changed)

Our objective in the four scenarios is to analyze the firm and consumer equilibrium decisions, linking them back to existing industry practices to provide practical managerial insights.

Figure 3 presents the results of four separate outcome variables from the simulation (panels a, b, c, d)[13]. In all graphs, the x-axis captures θ, the expected loss from a breach, while the y-axis captures η, the marginal cost of consumer effort. The z-axis represents ex ante firm investment (panel a), ex post firm investment (panel b), the ratio between ex ante investment and ex post firm investment (panel c), and level of consumer ex post effort (panel d).

Note that for illustration purposes, we reversed the axis for the consumer ex post effort (panel d, Figure 3). The four conditions of as shown in Table 1.

[13] Simulation parameters are the following: $\rho=4$, $\delta = 2$, $\gamma = 2$, $\alpha = 0.5$, $i= 5$.

Table 1 are reflected by four regions of the above graphs (θ low, η low; θ high, η low; θ low, η high; and θ high, η high). Each region is described in more detail below.

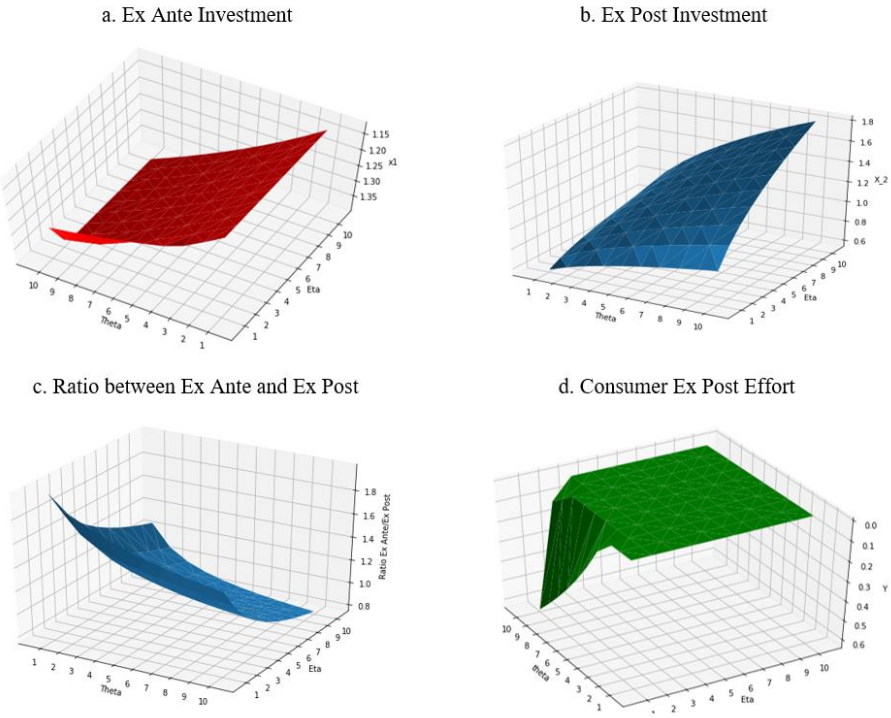

Figure 3: Simulation Results

θ low, η low: The breach involves low sensitivity information, and consumers can act. The firm invests both ex ante and ex post. Nevertheless, because the expected consumer loss is low, the firm's ex post investment will be lower than its ex ante investment. Additionally, even if it is not very costly for consumers to act, they will only do so as the expected loss starts increasing. For very low values of θ, consumers do not have incentive to invest at all, leaving the burden to the firm.

θ high, η low: The breach involves highly sensitive information, and consumers can act. The firm will have a similar incentive to invest ex ante and ex post, given the high expected loss. Consumers can act thanks to the low marginal cost of their activity, and have a great incentive to do so in the attempt to mitigate their relatively large expected loss.

θ low, η high: The breach involves low sensitivity information, and consumers cannot act. The firm will invest both ex ante and ex post. Nevertheless, because the expected consumer loss is low, the incentive to mitigate the consequences of the breach is low. As such, the ex ante investment will be higher than the ex post investment. For consumers, acting is not feasible due to the high marginal cost. As such, they will not intervene ex post.

θ high, η high: The breach involves highly sensitive information, but consumers cannot act. The firm is forced to bear all the burden of mitigating ex post losses, which are expected to be very high. As such, the incentive to invest ex post is very high, and so the firm invests more ex post than ex ante. For consumers, acting is not feasible due to the high marginal cost, and therefore will not intervene ex post.

We summarize the implications across the four scenarios in Table 2.

Table 2. Parameters Regions

	Low Sensitivity Information	**High Sensitivity Information**
Consumers can take action	θ low, η low. Ratio Ex Ante/Ex Post >>1 The firm has a greater incentive to invest ex ante rather than ex post because of low consumer loss. *Industry Example: Retail, and Utility sectors employing IoT devices*	θ high, η low. Ratio Ex Ante/Ex Post ~ 1. The firm has incentive to invest ex ante as well as ex post. *Industry Example: Financial (payment cards)*
Consumers cannot take action	θ low, η high. Ratio Ex Ante/Ex Post > 1. The firm has incentive to invest ex post due to consumers' inaction. But the expected consumer loss is low, so the amount invested ex post is lower than ex ante investments. *Industry Example: Online activities such as web browsing and social media behavior*	θ high, η high. Ratio Ex Ante/Ex Post < 0. The firm invests heavily ex post to mitigate the high expected consumer loss and compensate for consumers' inability to act. *Industry Example: Health/genetic information, and certain kinds of financial information involving detailed account and financial history*

Recall that the simulations held constant all parameters except η and θ. We describe here how the simulation results and the related graphs change as we individually vary 4 critical firm's parameters: firm liability (α), the firm's reputation cost (ρ), the firm's marginal cost of ex post and ex ante investments (δ, and γ, respectively).

1. *The firm responsibility changes with α.* Changes in α can be caused, for example, by a new regulation that expands or limits the definition of consumer harm following a data breach. For fixed values of the other parameters, as α decreases (increases), the ex post investment surface shifts down (up), causing the ratio between ex ante and ex post investment to increase (decrease). For relatively low (high) values of α, the ratio will always be greater (lower) than 1, leading the firm to always invest more (less) in the ex ante period, relative to the ex post period. The consumers' effort surface shifts down (up), extending (restricting) the parameter region where consumers invest a positive amount.
2. *The firm reputation cost changes with* ρ. Changes in ρ can be caused, for example, by reactions of the stock market. On one hand, the stock market may tend to react more strongly to breaches overtime; on the other, the stock market may tend to get de-sensitized overtime and react less strongly to breaches. For fixed values of the other parameters, as ρ increases (decreases), the ex post investment surface shifts up (down), causing the ratio between ex ante and ex post investment to decrease (increase). For relatively high (low) values of ρ, the ratio will always be less than (greater than) 1, and the firm will always invest less (more) in the ex ante period, relative to the ex post period . The consumers' effort surface shifts up (down), restricting (extending) the parameters region where consumers invest a positive amount.
3. *The firm's marginal cost of ex post investment changes with δ.* Changes in δ can be caused, for example, by changes in firm's efficiency. Small firms may be less cost-

efficient and face a higher δ compared to larger firms. For fixed values of the other parameters, as δ increases (decreases), it becomes costlier (cheaper) for the firm to invest ex post. The ex post investment surface shifts down (up) and becomes zero for very high values of δ. The ratio between ex ante and ex post investment shifts up, as ex ante investment is greater than ex post investment. The consumers' effort surface shifts down (up), extending (restricting) the parameters region where consumers invest a positive amount.

4. *The firm's marginal cost of ex ante investment changes with γ.* Changes in γ can be caused, for example, by technological improvements that reduce the cost of security technologies and investments. For fixed values of the other parameters, as γ increases (decreases), it becomes costlier (cheaper) for the firm to invest ex ante. The ex ante investment surface shifts downs (up) and the ratio between ex ante and ex post investments goes down, as ex ante investment decreases. Consumers' effort surface it is not affected by the change, as ex post parameters are independent from the ex ante ones.

The reported analysis highlights how the balance between investments in ex ante prevention and investments in ex post mitigation strongly depends on a number of factors that the firm should take into consideration, including: the nature of the data being protected, the regulatory environment, the ability of the consumers to act in response to a breach and, therefore, contribute to the mitigation efforts, the characteristics of the industry in which the firm operates. As such, firms should not necessarily assume that the more investments in ex ante prevention the better. Rather, if firm's budget in information security is limited, the decision on how to allocate this budget should follow optimality rules. Our analysis suggests that in certain situations it is optimal for the firm to invest a smaller amount ex ante and increase its ex post investment in mitigation activities if the breach occurs, for example when consumers cannot take meaningful action ex post or consumers can act but the breach involves highly sensitive information or a huge amount of records.

6. THE SOCIAL PLANNER'S PROBLEM

Having constructed a data breach accident model, we now examine how different policy interventions can affect aggregate welfare under the risk of data breaches.

6.1 Should companies be fined for data breaches?

Consider a policy maker who is interested in reducing the consequences of data breaches. How would imposing a fine on a firm that suffered a data breach affect firm and social outcomes? If the sanction were an immediate and exogenous addition to ex post costs – perhaps equal to the amount of consumer harm, it would represent, in principle, the Pigouvian (1932) approach to managing externalities – impose a tax on the injurer equal to the cost of the harm. The effect would be to raise overall ex post costs, but would not affect the amount of mitigation effort (x_2) because the firm would not consider this fine when minimizing ex post costs. However, it would increase ex ante effort (because total ex post costs are greater). Therefore, a fine would have the effect of increasing overall firm costs, drive it to take more preventive care to avoid a breach, but it would not affect the firm's behavior ex post.

This approach suffers from two issues: the amount of consumer harm caused by the breach (fraud, privacy invasion, increased interest rates, etc.) is often unknown, often unquantifiable, and small in magnitude. In general, it is difficult for consumers to fully compute the harm caused by data breaches. Moreover, because of the nature of identity theft, victims are often unable to uniquely identify the firm or breach which led to the harm.

Together, these characteristics suggest that, absent specific information regarding the cause and amount of harm, additional fines imposed on a firm would likely be suboptimal. Moreover, these conditions suggest that ex ante regulation, rather than information disclosure, could be a preferred policy instrument because of its ability to affect all firms across industries by enforcing a minimum level of security investment.

6.2 Social optimum at equilibrium levels of effort

Changes in firm and consumer costs will have two different and non-obvious effects on social welfare. For example, when a cost is shared between the firm and consumer (such as in the case of liability for loss), this will produce one distinct form of welfare outcome. On the other hand, as particular cost functions (e.g. disclosure or reputation) increase or decrease, aggregate costs will be affected in an entirely different manner, and discussed below.

As discussed, firms may bear substantial settlement costs because of a data breach lawsuit, and (Romanosky, 2014) show a large variation in the causes of action (legal theories brought) in breach lawsuits (including tort liability, breach of contract, violation of state and federal statutes, etc). Further, the disclosure costs borne by the firm can be substantial. While the cost may be endogenous to the firm, the requirement to bear such costs are a function of the disclosure requirements, which are driven by policy (i.e. the state laws requiring, or not, specific forms of notification, redress, or mitigating actions).

As shown in the left panel of Figure 4, an increase in the cost of disclosure, $d(x_2)$, raises aggregate costs for all values of ex post firm care while also increasing the socially optimal level of firm care (as shown by the upward direction of the arrow).[14] That is, as the cost to the firm of complying with disclosure increases, so do aggregate welfare costs, and thus the socially optimal level of data protection. On the other hand, as shown in the right panel of Figure 4, when the firm internalizes more consumer harm (as α increases), its marginal benefit of avoiding a data breach increases, raising its privately optimal level of care and it is driven to invest more closely to the socially optimal level of care ($\tilde{x}_B > \tilde{x}_A$).[15] Notice that this is achieved without change to the social cost function.

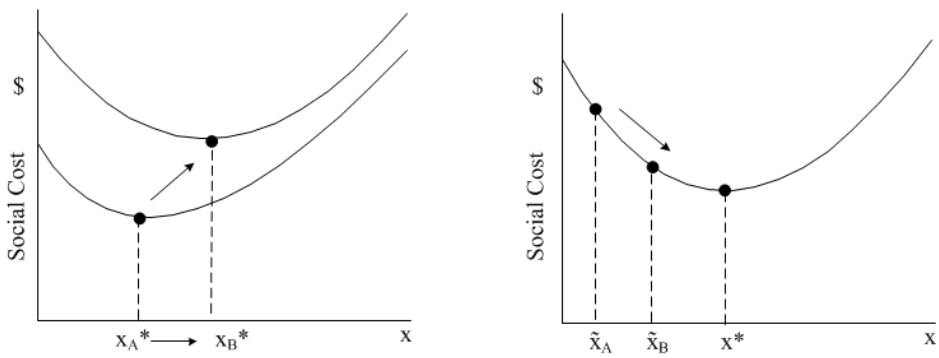

Figure 4: Movement of, and along, the social cost curve

Given the non-monotonic (uncertain) change in aggregate costs due to the amount of consumer harm internalized by the firm, and the opportunity for policy intervention to affect

[14] Notice also how the difference between the curves is largest at the vertical intercept (where the difference is equal to the change in the parameter values) and is decreasing in x (where the limit of the difference equals zero as x approaches infinity).

[15] This occurs because the change in α represents a transfer of cost between the firm and consumer. As mentioned, when α = 0, the consumer bears all damages from identity theft (the firm bears none), and when α= 1, the firm is strictly liable for consumer costs, causing the firm's cost-minimizing level of care to approach the socially optimal level of care.

this change through legislation and regulation, we therefore examine the conditions under which aggregate costs can be minimized at equilibrium levels of firm and consumer effort. It is important to also note that these privately optimal levels of firm and consumer care may not necessarily lead to the socially optimal solution (i.e., the levels of care that minimize aggregate costs). Intuitively, this is due to the fact that firms and consumers minimize their respective cost functions separately, and accounting only for the proportion of expected loss that they may bear. To give an example, there may be situations in which the firm could mitigate the consequences of the breach in a more effective way than consumers and therefore, from a social point of view, it would make sense for the firm to set a higher level of effort. Nevertheless, the level of effort required to minimize aggregate costs would be greater than the level of effort that the firm would set privately (exactly because the firm should increase its level of care to compensate for consumers' inefficiencies).

PROPOSITION 7. *The privately optimal levels of ex ante and ex post effort set by the firm and consumers,* $\tilde{x}_1$, $\tilde{x}_2$ *and* $\tilde{y}$ *are weakly lower than the socially optimal levels of effort,* x_1^*, x_2^*, y^*.

Proof is provided in the Appendix.

6.3 Should firms bear all consumer liability?

The extent to which a firm should bear more or less consumer harm is object of considerable debate. On one hand, many feel that the justice system fails when data breach lawsuits are promptly dismissed. On the other hand, in 2007, the governor of California vetoed a data breach bill on the grounds that firms already bore enough liability, stating that "the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers" (Schwararzenegger, 2007). Therefore, a second question that a policy maker might pose is: would forcing firms to fully compensate consumers for data breaches lead to a more efficient outcome? At first, one may assume that aggregate costs are minimized when the firm internalizes all consumer loss (i.e. as $\alpha \rightarrow 1$). This is the familiar Pigouvian tax solution (Pigou, 1932): achieve the socially efficient outcome by taxing the source of the harm an amount equal to the externality. However, this approach assumes unilateral care situations in which only one player (e.g. the firm) can prevent harm. Because our situation involves a bilateral care accident in which two players (the firm and consumer) can mitigate loss, the Pigouvian approach is not revealing. Further, the often cited-solution to bilateral care situations is that the efficient solution is achieved when the party with the greater marginal reduction in harm – the low cost avoider – prevents the loss (Coase, 1960) . Again, this approach is uninformative because it assumes that player actions are dichotomous (i.e. that a *single* action by either player could completely avoid the accident and eliminate the externality).[16] Because our situation involves a continuum of prevention activities by two parties (x_1, x_2, y), we must therefore employ more rigorous analytical solutions.

It can be shown that that minimal aggregate cost is achieved only when *both* the firm and consumer each bear some portion of consumer harm (and not just the firm). Indeed, there is an optimal value of liability assignment, $0 < \alpha^* < 1$, that minimizes the social cost. To do this, we note that social costs are *decreasing* in α when $\alpha = 0$ (no liability) and *increasing* in α when $\alpha = 1$ (strict liability). Not only does this imply that the social cost can be lowered by increasing firm liability when it bears none, or by decreasing liability when it bears all, but

[16] For example, to avoid a pedestrian slipping on an icy sidewalk, either the home owner should shovel the walkway, or the pedestrian should avoid the ice.

that there will be an optimal amount of firm liability that minimizes social costs. Complete proof are shown in the Appendix.

PROPOSITION 8. *When the social planner can control firm liability, there is a socially optimal level of liability that falls between strict and no liability. That is, there is an optimal value* $0 < \alpha^* < 1$ *which minimizes* $S(\alpha^*)$ *and satisfies the equation* $\partial S / \partial \alpha|_{\alpha = \alpha^*} = 0$.

Note that each party must contribute some effort to minimize aggregate costs, where the optimal portion of liability is driven by the marginal effectiveness of firm and consumer actions (i.e. the least cost avoider). We also recognize that the change in consumer behavior as a function of liability represents the substitutability of care (moral hazard): when the consumer is fully compensated for all loss, she has no incentive to take any precautions. Common law overcomes this problem by holding the injurer liable for damages unless the victim (consumer) is herself negligent (contributory negligence). For instance, causing a fire by recklessly operating a kitchen appliance. However, just as there has been no formally recognized duty of care on the part of firms to protect consumer information, there is also no established duty on the part of the consumer. Therefore, forcing firms to fully compensate consumers for data breaches, while arguably not an equitable solution, would not lead to an efficient outcome.

7. CONCLUSIONS

Data breaches are costly, and impose a significant burden on firms. Rational, cost-minimizing firms will seek ways to reduce overall breach costs, either through innovation and efficiency, investment in ex post mitigation. If it is true that most data breach costs are within the firm's control (i.e., not exogenously imposed by sanction), then it is reasonable to assume that the firm will have every incentive to reduce these costs. In this sense, the firm's incentive is aligned with the consumer's and the social planner's. If it is also true that the firm is in the better position to identify and reduce these costs, then this also suggests less need for government-imposed sanctions (*ex ante* regulation), and more opportunity for a light-handed (paternalistic) policy regime, such as information disclosure.

In this paper, we propose a novel framework to investigate the strategic interaction between a firm that invests in security and its consumers. The firm's dilemma is understanding how to balance ex ante investments in security protection, with ex post investments in mitigation activities in the case a breach occurs. But additionally, consumers themselves can act in order to mitigate their expected loss in the case of a security breach.

Our analysis produces several managerial insights. First, we find that under given conditions, a firm should not invest a considerable amount in ex ante prevention; rather, it should invest a smaller amount ex ante and increase its ex post investment in mitigation activities if the breach occurs. This happens in all the situations where: i) consumers cannot take meaningful action ex post, and the breach can have severe consequences on the firm either because the expected loss from the breach is high or the reputation cost for the cost is substantial; ii) consumers can act but the breach involves highly sensitive information or a huge amount of records. In this second case, the amount invested ex ante is very close to the amount invested ex post. Practical examples include breaches suffered by large companies (implying that the size of the breach is large), publicly traded companies whose reputation on the stock market may suffer because of a breach, and companies that manage highly sensitive data, such as health, biometric and certain kinds of financial information.

Second, there exist conditions under which the firm should optimally not invest *ex post*. This happens in all the situations where: i) consumers can feasibly act *ex post* and

contribute to the breach mitigation; ii) the expected loss from the breach is relatively low; or iii) the cost of ex post intervention for the firm is unreasonably high (due to firm's inefficiencies, for instance). Practical examples include breaches suffered by small companies, privately held or non-profit companies, and those that deal with low sensitivity data.

Finally, we find that, in order to minimize the social cost from a breach, consumers should always bear a positive proportion of the *ex post* expected loss. This result is particularly informative from a policy point of view as it suggests that social planners should never require companies to bear in full the consequences of a breach.

8. REFERENCES

[1] ABI: " High Profile Breaches Drive $1.7 Billion Data Loss Prevention Market in 2014", *ABI Research*, 2014. URL https://www.abiresearch.com/press/high-profile-breaches-drive-17-billion-data-loss-p.

[2] A. Acquisti, A. Friedman, R. Telang: "Is There a Cost to Privacy Breaches? An Event Study", , 2006.

[3] A. Arora: "Sell First, Fix Later: Impact of Patching on Software Quality", *Management Science (Research Note)* , pp. 465—471, 2006.

[4] A. Arora: "Competition and patching of security vulnerabilities: An empirical analysis", *Information Economics and Policy* , pp. 164—177, 2010.

[5] A. Arora: "An Empirical Analysis of Software Vendors Patch Release Behavior: Impact of Vulnerability Disclosure", *Information Systems Research* , pp. 115—132, 2010.

[6] A. Arora, H. Xu: "Optimal Policy for Software Vulnerability Disclosure", *Management Science*, pp. 642-656, 2007.

[7] BakerHostetler: "BakerHostetler Data Breach Chart", *BakerHostetler Data Breach Chart*, 2014. URL http://www.bakerlaw.com/files/Uploads/Documents/Data.

[8] J. Barth, J. Cordes: "Optimal Financial Disclosure With and Without SEC Regulation", *Quarterly Review of Economics and Business*, 1980.

[9] K. Baum: *Identity Theft, 2004*. Bureau of Justice Statistics, 2004.

[10] K. Baum: *Identity Theft, 2005*. Bureau of Justice Statistics, 2005.

[11] J. Brodkin: "ChoicePoint settles with 43 states over data breach", *Network World*, 2007. URL http://www.networkworld.com/news/2007/053107-choicepoint-settles-data-breach.html. [12] CIO: " 2013 State of the CIO", *CIO Magazine*, 2013. URL http://www.cio.com/documents/pdfs/2013.

[13] K. Campbell, L. Gordon, M. P. Loeb, L. Zhou: "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", *Journal of Computer Security*, pp. 431-448, 2003.

[14] H. Cavusoglu, H. Cavusoglu, H. Zhang: "Security Patch Management: Share the Burden or Share the Damage?", *Management Science*, pp. 657-670, 2008.

[15] H. Cavusoglu, B. Mishra, S. Raghunathan: "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", *International J. of Electronic Commerce*, 2004.

[16] H. Cavusoglu: “Decision-Theoretic and Game- Theoretic Approaches to IT Security Investment ”, *Journal of Management Information Systems*, 2008.

[17] A. Cezar: “Outsourcing Information Security: Contracting Issues and Security Implications ”, *Management Science* , 2014.

[18] L. Dignan: “What that data breach will really cost you.”, *ZDNet*, 2007. URL http://blogs.zdnet.com/BTL/?p=5007. Referencing Figure 1 reproduced from Forrester Research.

[19] Federal Trade Commission: *2006 Identity Theft Survey Report*. Federal Trade Commission, 2003.

[20] Federal Trade Commission: *2006 Identity Theft Survey Report*. Federal Trade Commission, 2007.

[21] A. Fung, M. Graham, D. Weil: *Full Disclosure: The Perils of and Promise of Transparency*. Cambridge University Press, 2007.

[22] GAO: *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737*. Government Accountability Office, 2007.

[23] N. Gandal, J. Choi, C. Fershtman: “Network Security: Vulnerabilities and Disclosure Policy”, *Journal of Industrial Economics*, 2009. forthcoming.

[24] Gartner: “Gartner Says Worldwide Security Market to Grow 8.7 Percent in 2013”, *Gartner Inc*, 2013. URL http://www.gartner.com/newsroom/id/2512215.

[25] G. Gordon, J. Rebovich, K. Choo, J. Gordon: “Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement”, *Center for Identity Management and Information Protection*, 2007. Utica College.

[26] L. A. Gordon, P. L. Martin, W. Lucyshyn, T. and Sohail: “The Impact of the Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities”, *Journal of Accounting and Public Policy*, pp. 503-530, 2006.

[27] Lawrence A. Gordon, Martin P. Loeb: “The Economics of Information Security Investment”, *ACM Trans. Inf. Syst. Secur.*, pp. 438—457, 2002.

[28] M. Greisiger: “ Cyber Liability and Data Breach Insurance Claims”, *NetDiligence* , 2012. URL http://www.netdiligence.com/files/CyberClaimsStudy-2012sh.pdf.

[29] J. Grossklags, N. Christin, J. Chuang: “Secure or Insure? A Game-Theoretic Analysis of Information Security Games”, *In Proceedings of the 17th International World Wide Web Conference, Beijing, China*, pp. 209-218, 2008.

[30] E. Harrell: “Victims of Identity Theft, 2012”, *Bureau of Justice Statistics, U.S. Department of Justice*, 2014. URL http://www.bjs.gov/content/pub/pdf/vit12.pdf.

[31] C. Hoffman, C. Shih: “What Is Expedient Notification Of A "Data Breach?”, *Mondaq Business Briefing*, 2014. URL http://http://www.mondaq.com/unitedstates/x/294034/data+protection/What+is+Expedient+Notification+of+a+Data+Breach.

[32] Hogan, Lovells: “ Data Breaches: Time for High Alert, Avoiding and Managing the Legal Risks of Cybersecurity Incidents”, *Hogan and Lovells*, 2014. URL http://www.hldataprotection.com/2014/03/articles/cybersecurity-data-breaches/upcoming-hogan-lovells-webcast-will-address-data-breach-preparedness-and-response/.

[33] Infosec: “ Global security spending to hit 86B in 2016”, *InfoSecurity Magazine* , 2012. URL http://http://www.infosecurity-magazine.com/view/28219/global-security-spending-to-hit-86b-in-2016/.

[34] Javelin Strategy, Research: “Identity Fraud Survey Report”, , 2006. Consumer Version.

[35] Javelin Strategy, Research: “Identity Fraud Survey Report”, , 2009. Consumer Version.

[36] G. Jin, P. Leslie: “The Effect of Information on Product Quality: Evidence from Restaurant Hygiene Grade Cards”, *Quarterly Journal of Economics*, pp. 409-451, 2003.

[37] K. Kannan, J. Rees, S. Sridhar: “Market Reactions to Information Security Breach Announcements”, *International Journal of Electronic Commerce*, pp. 69-91, 2007.

[38] D. Kaplan: “Heartland settles with Discover over breach”, *SC Magazine*, 2010. URL http://www.scmagazine.com/heartland-settles-with-discover-over-breach/article/178116/.

[39] M. Kingston: “Written Testimony of Michael R. Kingston”, *Senate Judiciary Committee February 4, 2014, Hearing On Privacy In The Digital Age: Preventing Data Breaches And Combating Cybercrime*, 2014. URL http://www.judiciary.senate.gov/imo/media/doc/02-04-14KingstonTestimony.pdf.

[40] J. Kirk: “ How much should you spend on IT security?”, *Computerworld*, 2010. URL http://www.computerworld.com/s/article/9187239/How_much_should_you_spend_on_IT_security_.

[41] C. Kolstad, T. Ulen, G. Johnson: “Ex Post Liability for Harm vs. Ex Ante Safety Regulation: Substitutes or Complements?”, *American Economic Review, American Economic Association*, pp. 888-901, 1990.

[42] W. Landes, R. Posner: *The Economic Structure of Tort Law*. Harvard University Press, 1987.

[43] S. Laube: “The Economics of Mandatory Security Breach Reporting to Authorities ”, *WISE* , 2015.

[44] Y. J. Lee: “Profit-maximizing firm investments in customer information security”, *Decision Support Systems*, pp. 904—920, 2011.

[45] R. Lemos: “TJX estimates breach costs at $118 million”, *Security Focus*, 2009. URL http://www.securityfocus.com/brief/568.

[46] D. Lui: “Knowledge sharing and investment decisions in information security ”, *Decision Support Systems*, pp. 95—107, 2011. [47] D. Majoras: “Prepared Statement Of The Federal Trade Commission Before The Committee On Commerce, Science, And Transportation U.S. Senate On Data Breaches And Identity Theft, June 16, 2005”, , 2005.

[48] A. Maurushat: “Data Breach Notification Law Across the World from California to Australia”, *University of New South Wales Faculty of Law Research Series*, 2009. URL http://law.bepress.com/cgi/viewcontent.cgi?article=1153&context=unswwps.

[49] M. McGrath: “Target Profit Falls 46”, *Forbes* , 2014. URL http://http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/.

[50] J. Mulligan: “Written Testimony of John Mulligan”, *Senate Judiciary Committee February 4, 2014, Hearing On Privacy In The Digital Age: Preventing Data Breaches And Combating Cybercrime*, 2014. URL http://www.judiciary.senate.gov/imo/media/doc/02-04-14MulliganTestimony.pdf.

[51] NIST: “Framework for Improving Critical Infrastructure Cybersecurity”, *National Institute of Standards and Technology*, 2014. URL http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.

[52] Orrick: “ Targeting Harm From A Breach: Plaintiffs Lawyers Get Creative In Data Privacy Suits”, *Orrick, Herrington and Sutcliffe LLP.* , 2014. URL http://http://www.mondaq.com/unitedstates/x/293800/Data+Protection+Privacy/Washington+Legal+Foundations+Legal+Backgrounder+Targeting+Harm+From+A+Breach+Plaintiffs+Lawyers+Get+Creative+In+Data+Privacy+Suits.

[53] A. Ozdaglar: “ Game Theory with Engineering Applications Lecture 6: Continuous and Discontinuous Games”, *MIT Course 6.254* , 2010. URL http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-254-game-theory-with-engineering-applications-spring-2010/lecture-notes/MIT6_254S10_lec06.pdf.

[54] Arthur C. Pigou: *The Economics of Welfare*. Library of Economics and Liberty, 1932.

[55] Ponemon: *2011 Annual Study: Cost of a Data Breach*. The Ponemon Institute, 2011.

[56] Ponemon: “2013 Cost of Data Breach Study: Global Analysis”, *Ponemon Institute LLC*, 2013.

[57] D. Pulliam: “VA sets aside $20 million to handle latest data breach”, *Government Executive*, 2007. URL http://www.govexec.com/story_page.cfm?articleid=37191&dcn=todaysnews.

[58] T. Robinson: “ Class-action suit aimed at MCCCD for delayed notification in breach”, *SCMagazine Online*, 2014. URL http://www.scmagazine.com/class-action-suit-aimed-at-mcccd-for-delayed-notification-in-breach/article/343569/.

[59] S. Romanosky: “Empirical Analysis of Data Breach Litigation”, *Journal of Empirical Legal Studies*, pp. 74-104, 2014.

[60] S. Romanosky: “Do Data Breach Disclosure Laws Reduce Identity Theft?”, *Journal of Policy Analysis and Management*, pp. 256-286, 2011.

[61] A. Schwarzenegger: “Letter to the members of the California State Assembly”, , 2007. URL http://gov.ca.gov/pdf/press/2007bills/AB.

[62] S. Shavell: “A Model of the Optimal Use of Liability and Safety Regulation”, *The RAND Journal of Economics*, pp. 271-280, 1984.

[63] TJX: “The TJX Companies, Inc. Reports Strong Second Quarter FY08 Operating Results, Estimates Liability from Computer Systems Intrusion(s)”, *Press Release TJX Companies*, 2007. URL http://investor.tjx.com/phoenix.zhtml?c=118215&p=irol-newsArticle&ID=1040186&highlight=.

[64] R. Telang, S. Wattal: “An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price”, *IEEE Transactions on Software Engineering paper*, pp. 544-557, 2007.

[65] Tom Coburn: “The Federal Governments Track Record on Cybersecurity and Critical Infrastructure”, *A report prepared by the Minority Staff of the Homeland Security and Governmental Affairs Committee*, 2014. URL http://www.coburn.senate.gov/public/index.cfm?a=Files.Serve&File_id=f1d97a51-aca9-499f-a516-28eb872748c0.

[66] Trustwave: “Trustwave Global Security Report 2013”, *Trustwave*, 2014. URL http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

[67] R. Verrecchia: “Essays on Disclosure”, *Journal of Accounting and Economics*, pp. 97-180, 2001.

[68] T. Wang, J. Rees, K. Kannan: “The Impact of Information Security Disclosures on Market Reactions to Security Breaches”, , 2009. under review.

[69] R. Westervelt: “Investment In Data Breach Responders Lacking, Study Finds”, *CRN Online*, 2014. URL http://www.crn.com/news/security/300071737/investment-in-data-breach-responders-lacking-study-finds.htm.

[70] F. Wolf: “Recent Case Opens the Door for Data Breach Class Actions”, *Kroll Cyber Security Blog*, 2011. URL http://www.krollfraudsolutionsblog.com/2011/11/recent-case-opens-the-door-for-data-breach-class-actions/.

[71] D. Yadron: “Companies Wrestle With the Cost of Cybersecurity”, *The Wall Street Journal*, 2014. URL http://online.wsj.com/news/articles/SB10001424052702304834704579403421539734550.

9. APPENDIX

9.1Proof of Existence

Detailed proofs of existence and uniqueness of an equilibrium, in the case of diagonally strictly concave games, are given in [53] and Rosen (1965). In these sources, the problem is formulating in terms of payoff maximization. In our case, we formulate the problem in terms of cost minimization, and consequently the relevant theorems must be framed in terms of convexity.

For our game, existence of an equilibrium follows from recognizing that the scenario is a continuous, 2-player game with bounded strategy sets. User and firm activity are non-negative and, for practical purposes, finite. The proof is an application of Glicksberg’s theorem (Ozdaglar, 2010, slide 4).

The convexity of the cost functions is not enough on its own to guarantee uniqueness (Ozdaglar, 2010, provides an example on slide 21); however, if a stronger property, strict diagonal convexity, holds, then the solution is unique. The cost functions are strictly diagonally convex if

$$(X - X')^T \nabla u(X') - (X - X')^T \nabla u(X) < 0$$

where $X = (x_2, y)$, $X' = (x_2', y')$ are both solutions included in the strategy set, and $u = (F(x_2), C(y))$.

To demonstrate strict diagonal convexity, it is sufficient to show that $U + U^T$ is negative definite where U is the Jacobian of ∇u.

Note that the optimal values of x_2 and y do not depend on the value of x_1, therefore it is sufficient to demonstrate strict diagonal convexity in the ex post portion of the game alone. The existence of a unique optimal value of x_1 is clear from the convexity of F once the equilibrium values of x_2 and y are determined.

9.2 Proof of Lemma 1

We have the following cost functions:

$F(x_1, x_2, y) = \gamma x_1 + (1)/((1 + x_1))[i + \delta x_2 + (\rho)/((1 + x_2)) + \alpha(\theta)/((1 + x_2)(1 + y))]$

$C(x_2, y) = (1)/((1 + x_1))[\eta x_2 + (1 - \alpha)(\theta)/((1 + x_2)(1 + y))]$

To find the optimal level of x_2 , we solve for the first order condition of the firm's total cost function with respect to x_2:

$(\partial F)/(\partial x_2) = (1)/((1 + x_1))[\delta - (\rho)/((1 + x_2)^2) - (\alpha\theta(1 + y))/((1 + x_2)^2(1 + y)^2)]$

$(1)/((1 + x_1))[\delta - (\rho)/((1 + x_2)^2) - (\alpha\theta)/((1 + x_2)^2(1 + y))]$

Solving for x_2, we obtain: $x_2 = -1 \pm \sqrt{(\rho + \alpha\theta)/\delta(1 + y)}$

By assumption, investments can never be negative; as such, we consider only the non-negative root. Therefore, we have that: $\tilde{x}_2 = \sqrt{\frac{1}{\delta}(p + \frac{\alpha\theta}{(1+y)})} - 1$

Similarly, to find the optimal amount of consumers' effort, y , we solve for the first order condition of consumers' total cost function with respect to y:

$(\partial C)/(\partial y) = (1)/((1 + x_1))[\eta - ((1 - \alpha)\theta(1 + x_2))/((1 + x_2)^2(1 + y)^2)]$

$(1)/((1 + x_1))[\eta - ((1 - \alpha)\theta(1 + x_2))/((1 + x_2)^2(1 + y)^2)] = 0$

Solving for y, we obtain: $y = -1 \pm \sqrt{(1 - \alpha)\theta/\eta(1 + x_2)}$

Since we assume that consumers' effort is non-negative, we have that:

$$\tilde{y} = \sqrt{(1 - \alpha)\theta/\eta(1 + x_2)} - 1$$

Finally, once we have the solutions for x_2 and y ,we can plug them back into the firm's cost function and find the solution for x_1:

$F(x_1, \tilde{x}_2, \tilde{y}) = \gamma x_1 + 1/(1 + x_1)[i + \delta\left(\sqrt{\frac{1}{\delta}\left(p + \frac{\alpha\theta}{(1+y)}\right)} - 1\right) + \rho/\sqrt{\frac{1}{\delta}\left(p + \frac{\alpha\theta}{(1+y)}\right)} + \alpha\theta/(\sqrt{\frac{1}{\delta}\left(p + \frac{\alpha\theta}{(1+y)}\right)}(1 + y)\ )$

By taking the derivate with respect to x_1 and solving, we obtain:

$$\tilde{x}_1 = \sqrt{\frac{1}{\gamma}[i - \delta + 2\sqrt{\delta}\sqrt{(p + \frac{\alpha\theta}{(1 + \tilde{y})})} - 1}$$

9.3Proof of Lemma 2

Assume that in equilibrium $\tilde{x}_2 = 0$. This implies that it must be the case that: $\sqrt{\frac{1}{\delta}(p + \frac{\alpha\theta}{(1+\tilde{y})})} \leq 1$. In turns, this requires $\tilde{y} \geq (\alpha\theta)/(\delta - \rho) - 1$.

Symmetrically, if $\tilde{x}_2 = 0$, then $\tilde{y} = \sqrt{\frac{(1-\alpha)\theta}{\eta}} - 1$.

As a consequence, when $\sqrt{\frac{(1-\alpha)\theta}{\eta}} \geq \frac{\alpha\theta}{\delta-\rho}$, $\tilde{x}_2 = 0$ and $\tilde{y} \geq 0$.

Similarly, let us assume that in equilibrium $\tilde{y} = 0$. This implies that it must be that:

$\sqrt{(1-\alpha)\theta/\eta(1+x_2)} \leq 1$. In turns, this requires $\tilde{x}_2 \geq \frac{(1-\alpha)\theta}{\eta} - 1$.

Symmetrically, if $\tilde{y} = 0$ then $\tilde{x}_2 = \sqrt{\frac{1}{\delta}(p+\alpha\theta)} - 1$.

Therefore, when $\sqrt{\frac{1}{\delta}(p+\alpha\theta)} \geq \frac{(1-\alpha)\theta}{\eta}$, then $\tilde{x_2} \geq 0$ and $\tilde{y} = 0$.

9.4 Proof for Lemma 3

It follows from solving the following:

$$\sqrt{\frac{1}{\gamma}[i-\delta+2\sqrt{\delta}\sqrt{(p+\frac{\alpha\theta}{(1+\tilde{y})})}} - 1 < \sqrt{\frac{1}{\delta}(p+\frac{\alpha\theta}{(1+y)})} - 1$$

Rearranging, we find: $\sqrt{\delta}\frac{(i-\delta)}{(\gamma-2\delta)} < \sqrt{\rho+\frac{\alpha\theta}{(1+\tilde{y})}}$

9.5 Proof for PROPOSITION 1

As the cost of disclosure decreases, firms will increase their level of ex post effort in order to mitigate the consequences of a breach. If $\tilde{d}(x_2) = ad(x_2) + b < d(x_2)$ for all x_2, where a and b are constants, then $\tilde{x}_2 > x_2$ given y.

Proof. First, we note that the structure of $\tilde{d}$ implies that $a \in (0, 1)$, otherwise either the inequality or one of the properties of a cost function would be violated. This implies that the derivative $\tilde{d}'(x_2) = ad'(x_2) < d'(x_2)$ for all x_2. The condition for optimal firm effort before costs drop is

$\partial_{x2}F(\tilde{x}_2) = p_B(d'(\tilde{x}_2) + r'(\tilde{x}_2) + \alpha\partial_{x2}H(\tilde{x}_2, y)) = 0$

so that,

$\tilde{d}'(\tilde{x}_2) + r'(\tilde{x}_2) + \alpha\partial_{x2}H(\tilde{x}_2, y) < d'(\tilde{x}_2) + r'(\tilde{x}_2) + \alpha\partial_{x2}H(\tilde{x}_2, y) = 0$

$\tilde{d}'(\tilde{x}_2) < -(r'(\tilde{x}_2) + \alpha\partial_{x2}H(\tilde{x}_2, y))$

Recall that $\tilde{d}$ is increasing and r and H are decreasing in x_2, so it is necessary to increase the value of x_2 in order to achieve equality. Therefore, $\tilde{x}_2 > x_2$.

9.6 Proof for PROPOSITION 2

As reputation costs decrease, firms will decrease their level of ex post mitigation effort. If $\tilde{r}(x_2) = ar(x_2) < r(x_2)$ for all x_2 where $0 < a < 1$, then $\tilde{x}_2^* < x_2^*$ given y.

Proof. First note that we do not include a constant term b because $\lim_{x2\to\infty} r(x_2) = 0$ applied to $\tilde{r}(x_2)$ would imply $b = 0$. Since reputation costs are decreasing we have $\tilde{r}'(x_2) = ar'(x_2) > r'(x_2)$ for all x_2. The condition for optimal firm effort before costs drop is

$\partial_{x2}F(\tilde{x}_2) = p_B(d'(\tilde{x}_2) + r'(\tilde{x}_2) + \alpha\partial_{x2}H(\tilde{x}_2, y)) = 0$

so that,

$d'(\tilde{x}_2) + \tilde{r}'(\tilde{x}_2) + \alpha\partial_{x2}H(\tilde{x}_2, y) > d'(\tilde{x}_2) + r'(\tilde{x}_2) + \alpha\partial_{x2}H(\tilde{x}_2, y) = 0$

$d'(\tilde{x}_2) > -(\tilde{r}'(\tilde{x}_2) + \alpha\partial_{x2}H(\tilde{x}_2, y))$

Recall that d is increasing and $\tilde{r}$ and H are decreasing in x_2, so it is necessary to decrease the value of x_2 in order to achieve equality. Therefore, $\tilde{x}_2 < x_2$. The same reasoning can be applied when $\hat{H}(x_2, y) = aH(x_2, y) < H(x_2, y)$, and again we have that $\tilde{x}_2 < x_2$.

9.7 Proof for PROPOSITION 3

As breach prevention technologies become cheaper, firms will invest more and enjoy lower total costs. If $\tilde{c}(x_1) = ac(x_1) + b < c(x_1)$ for all x_1 where a and b are constants, then $\tilde{x}_1 > x_1$ and $F(\tilde{x}_1, x_2, y) < F(x_1, x_2, y)$.

Proof. First, we note that x_2 and y are independent of the value of x_1, $c(x_1)$, and $p_B(x_1)$. The same argument as made in the previous propositions applies again, leading to the conclusion that pre-breach firm effort increases, $\tilde{x}_1 > x_1$.

Since the values x_2 and y are constant as prevention techniques become cheaper, it is straightforward to show that the total firm cost will also decrease,

$$\begin{aligned}
&\tilde{c}(\tilde{x}_1) + P_b(\tilde{x}_1)(i + d(x_2) + r(x_2) + \alpha H_{ID}(x_2, y)) < \\
&\tilde{c}(x_1) + P_b(x_1)(i + d(x_2) + r(x_2) + \alpha H_{ID}(x_2, y)) = \\
&ac(x_1) + b + P_b(\tilde{x}_1)(i + d(x_2) + r(x_2) + \alpha H_{ID}(x_2, y)) < \\
&c(x_1) + P_b(x_1)(i + d(x_2) + r(x_2) + \alpha H_{ID}(x_2, y)).
\end{aligned}$$

9.8 Proof for PROPOSITION 4

The decrease in effort is shown in the same manner as the decrease in effort in Proposition 2, and the lower overall costs are shown in the same manner as in Proposition 3.

9.9 Proof for PROPOSITION 5

As the cost of ex post consumer mitigation activities increases, consumers will decrease their level of ex post effort. If $\tilde{h}_{TE}(y) = ah_{TE}(y) + b > h_{TE}(y)$ for all y, where a and b are constants, then $\tilde{y} < y$ given x_2.

Proof. First, we note that the structure of $\tilde{h}_{TE}$ implies that $a \in (0, 1)$, otherwise either the inequality or one of the properties of a cost function would be violated. This implies that the derivative $\tilde{h}_{TE}'(y) = ah_{TE}'(y) > h_{TE}'(y)$ for all y. The condition for optimal consumers' effort before costs increase is $\partial_y C(y) = p_B(x_1)(h'_{TE}(y) + (1 - \alpha)\, \partial_y H(x_2, y)) = 0$

so that $\tilde{h}'(\tilde{y}) + (1 - \alpha)\partial_y H(x_2, \tilde{y}) > h'_{TE}(y) + (1 - \alpha)\, \partial_y H(x_2, y) = 0$

$\tilde{h}'(\tilde{y}) > -((1 - \alpha)\partial_y H(x_2, \tilde{y}))$

Recall that $h_{T\tilde{E}}$ is increasing and H is decreasing in y, so it is necessary to decrease the value of y in order to achieve equality. Therefore, $\tilde{y} < y$.

9.10 Proof for PROPOSITION 6

Proof. First note that we do not include a constant term b because $\lim_{y \to \infty} H(x_2, y) = 0$ applied to $\hat{H}(x_2, y)$ would imply $b = 0$. Since expected loss is decreasing we have $\partial_y \hat{H}(x_2, y) = a\partial_y H(x_2, y) > \partial_y H(x_2, y)$ for all y. The condition for optimal consumers' effort before the drop is $\partial_y C(y) = p_B(x_1)(h'_{TE}(y) + (1 - \alpha)\, \partial_y H(x_2, y)) = 0$

so that $h'_{TE}(y) + (1 - \alpha)\, \partial_y \tilde{H}(x_2, y) > h'_{TE}(y) + (1 - \alpha)\, \partial_y H(x_2, y) = 0$

$h'_{TE}(y) > -((1 - \alpha)\, \partial_y \tilde{H}(x_2, y))$

Recall that h is increasing and H is decreasing in y, so it is necessary to decrease the value of y in order to achieve equality. Therefore, $\tilde{y} < y$.

9.11 Proof for PROPOSITION 7

Let us start by considering the optimization problem of the firm and consumers when they set their private level of optimal effort. In the second period, the firm sets $\tilde{x}_2$ such that:

$$(7.1)\ d'(\tilde{x}_2) = -[r'(\tilde{x}_2) + \alpha\partial_{x2}H(\tilde{x}_2, y)]$$

and it sets $\tilde{x}_1$, in the first period, such that:

$$(7.2)\ c'(\tilde{x}_1) = -P_b(\tilde{x}_1)[i + d(\tilde{x}_2) + r(\tilde{x}_2) + \alpha H(\tilde{x}_2, y)]$$

Similarly, consumers set $\tilde{y}$ such that:

$$(7.3)\ h'_{TE}(\tilde{y}) = -[(1-\alpha)\partial_y H(x_2, \tilde{y})]$$

Differently, a social planner would set the levels of x_1^*, x_2^*, y^*so to minimize:

$$(7.4)\ S(x_1, x_2, y) = c(x_1) + P_b(x_1)[i + d(x_2) + r(x_2) + h_{TE}(y) + H(x_2, y)]$$

Therefore, the first order conditions become:

$$(7.5)\ d'(x_2^*) = -[r'(x_2^*) + \partial_{x2}H(x_2^*, y)]$$

$$(7.6)\ h'_{TE}(y^*) = -[\partial H(x_2, y^*)]$$

The main difference between Eq. 7.1 and Eq. 7.5 is given by the term $\alpha\partial_{x2}H(x_2, y)$. Comparing the two equations, we have that:

$$d'(x_2) = -[r'(x_2) + \alpha\partial_{x2}H(x_2, y)] \leq -[r'(x_2) + \partial_{x2}H(x_2, y)]$$

as $\alpha\partial_{x2}H(x_2, y) \leq \partial_{x2}H(x_2, y)$ because $0 \leq \alpha \leq 1$.In addition d' is increasing in $x_2$while $\partial_{x2}H$ is decreasing; this implies that the level of x_2 needed to reach equality in Eq. 7.5 is greater than the level of x_2 needed to reach equality in Eq. 7.1. Consequently, we have that $x_2^* \geq \tilde{x}_2$. The same reasoning can be applied for y and x_1.

9.12 Proof for PROPOSITION 8

The optimal value of α is that which minimizes the social cost evaluated at the NE solution. For convenience, let us write the cost functions as

$$(8.1)\ F = c + p_b(i + d + r + \alpha H)$$

$$(8.2)\ C = p_b(h_t + (1-\alpha)H)$$

$$(8.3)\ S = c + p_b(i + d + r + \alpha H) + p_b(h_t + (1-\alpha)H)$$

To find the value of α that minimizes S, set: $(dS)/(d\alpha) = 0$

$$(8.4)\ 0 = c'\partial_\alpha x_1 + p_b'\partial_\alpha x_1\,(i + d + r + \alpha H) + p_b(d'\partial_\alpha x_2 + r'\partial_\alpha x_2 + H + \alpha(\partial_\alpha x_2 + \partial_\alpha y)H)$$

$$+ p_B'\partial_\alpha x_1(h_t + (1-\alpha)H) + p_B(h_t'\partial_\alpha x_2 - H + (1-\alpha)(\partial_\alpha x_2 + \partial_\alpha y)H)$$

$$= (c' + p_b'(i + d + r + h_t + H))\partial_\alpha x_1 + p_B(d' + r' + \partial_{x2}H)\partial_\alpha x_2 + p_B(h_T' + \partial_y H)\partial_\alpha y$$

Next, find $\partial_\alpha x_1$, $\partial_\alpha x_2$, and $\partial_\alpha y$. Note that $\partial_\alpha x_1$ is the change in the NE value of x_1 as α varies. Since the NE value of x_1 satisfies $(\partial F)/(\partial x_1) = 0$, we have that:

(8.5) $(\partial)/(\partial\alpha)[(\partial F)/(\partial x_1) = 0]$

(8.6) $(\partial)/(\partial\alpha)[c' + p_B'(i + d + r + \alpha H) = 0]$

$(c'' + p_B''(i + d + r + \alpha H))\partial_\alpha x_1 + p_B'(d' + r' + \alpha\partial_{x2}H)\partial_\alpha x_2 \quad + (p_B'\alpha\partial_y H)\partial_\alpha y + p_B'H = 0$

so that:

(8.7) $d_\alpha x_1 = (- p_B'H - (p_B'\alpha\partial_y H)\partial_\alpha y - p_B'(d' + r' + \alpha\partial_{x2}H)\partial_\alpha x_2)/(c'' + p_B''(i + d + r + \alpha H))$

Similarly, we solve for $\partial_\alpha y$ and $\partial_\alpha x_2$

(8.8) $(\partial)/(\partial\alpha)[(\partial F)/(\partial x_2) = 0]$

(8.8) $(\partial)/(\partial\alpha)[p_B(d' + r' + \alpha\partial_{x2}H) = 0]$

(8.10) $(d'' + r'' + \alpha\partial_{x2}{}^2H)\partial_\alpha x_2 + (\partial_{x2}H + \alpha\partial_{x2y}{}^2H\partial_\alpha y) = 0$

(8.11) $(d'' + r'' + \alpha\partial_{x2}{}^2H)\partial_\alpha x_2 + (\alpha\partial_{x2}{}^2yH)\partial_\alpha y = -\partial_{x2}H$

Noting that $\partial_\alpha x_1$ does not appear in the equations for $\partial_\alpha x_2$ and $\partial_\alpha y$, we can solve for the later variables first, then plug in the solution to find $\partial_\alpha x_1$.

Step 1: Solve for $[\ \partial_\alpha x_2 \quad \partial_\alpha y\ ]$

(8.12)$[\ d'' + r'' + \alpha\partial_{x2}{}^2H\ \alpha\partial_{x2y}{}^2H\ (1 - \alpha)\partial_{x2y}{}^2H\ h_T'' + (1 - \alpha)\partial_y{}^2H\ ][\ \partial_\alpha x_2 \quad \partial_\alpha y\ ]$

$= [\ \partial_{x2}H \quad \partial_y H\ ]$

Step 2: Plug result in to find:

(8.13)
$\partial_\alpha x_1 = -(p_B'H + (p_B'\alpha\partial_y H)\partial_\alpha y + p_B'(d' + r' + \alpha\partial_{x2}H)\partial_\alpha x_2)/(c'' + p_B''(i + d + r + \alpha H))$

that becomes:

(8.14) $\partial_\alpha x_1 = -(p_B'(H + \alpha\partial_Y H\partial_\alpha y))/(c'' + p_B''(i + d + r + \alpha H))$

(8.15) $[\ \partial_\alpha x_2 \quad \partial_\alpha y\ ] = ([\ h_T'' + (1 - \alpha)\partial_y{}^2H \ \ -\alpha\partial_{x2y2H} - (1 - \alpha)\partial_{x2y}{}^2H\ d'' + r'' + \alpha\partial_{x2}{}^2H\ ][\ -\partial_{x2}H \quad -\partial_y H\ ])/(C)$

where $C = (h_T'' + (1 - \alpha)\partial_y{}^2H)(d'' + r'' + \alpha\partial_{x2}{}^2H) - (1 - \alpha)\alpha(\partial_{x2y}{}^2H)^2$

Step 3. Finally, substitute the values for $\partial_\alpha x_1$, $\partial_\alpha x_2$, and $\partial_\alpha y$ into equation 8.4 and find the optimal value for α.

9.13 Tables

A summary of variables used in the model is shown in Table 3, and a summary of the equations representing expected firm, consumer, and aggregate costs both is shown in Table 4.

Table 3. Summary of variables

Variable	**Description**

$x_1,\ x_2,\ y$	Level of ex ante prevention (firm), ex post mitigation (firm), and consumer effort
$c(x_1)$	Cost of ex ante prevention controls
$p_B(x_1)$	Probability of a data breach
i	Cost of investigating a data breach
$d(x_2),\ r(x_2)$	Disclosure cost, and reputation cost
$H_{ID}(x_2, y),\ h_{TE}(y)$	Expected consumer loss from identity theft, and consumer cost of time & effort
α	Portion of consumer costs born by the firm (firm liability)
$\tilde{x}_1, \tilde{x}_2,\ \tilde{y}$	Nash equilibrium levels of ex ante and ex post firm care, and consumer care
$x_1^*, x_2^*,\ y$	Socially optimal levels of ex ante and ex post firm care, and consumer care
$F(x_1, x_2), C(y), S(x_1, x_2, y)$	Firm, consumer, and social cost functions

Table 4. Summary of Cost Functions

Party	**Cost function**
Firm	$c(x_1) + p_B(x_1)(i + d(x_2) + r(x_2) + \alpha\ H_{ID}(x_2, y))$
Consumer	$p_B(x_1)(h_{TE}(y) + (1 - \alpha)\ H_{ID}(x_2, y))$
Social	$c(x_1) + p_B(x_1)(i + d(x_2) + r(x_2) +\ H_{ID}(x_2, y) + h_{TE}(y))$