Submitted to *Law and Econ of Data Security Policy, GMU, 5/17/2014*

DRAFT: Public disclosure of data breaches: optimizing ex ante and ex post security investments

In order to reduce the harms caused by data breaches, most states across the U.S. have enacted laws requiring organizations to notify individuals when their personal information has been lost or stolen. While these laws are intended to help reduce consumer identity theft, they also impose numerous costs on firms. For example, the requirement to publicly disclose a breach is itself costly, which in turn exposes the firm to reputation losses and consumer litigation. Therefore, in order to reduce the cost of data breaches in the face of recent disclosure requirements, firms are faced with competing alternatives. On one hand, complete investment in ex ante measures may help prevent a breach, but this is inefficient and impractical. On the other hand, ex post mitigation efforts may help avoid some losses, but would not prevent the breach from occurring in the first place. By applying the economic analysis of accident law to an information technology problem, we model a 2-period, 2-player game in which the firm strategically decides between ex ante security controls, and ex post mitigation efforts. Based on these investments, consumers also determine their level of identity theft protection. We solve for the optimal level ex post and ex ante investments, and examine how firm behavior is affected by public disclosure laws. We also analyze social costs to determine the amount of consumer liability that a firm should optimally internalize.

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

We would like to thank the Law and Economics Center at George Mason University School of Law and CyLab at Carnegie Mellon University for their generous support, as well as Nicolas Christin and participants of the Ninth Workshop on the Economics of Information Security and participants of George Mason Law and Economics Seminar on Economics of Data Security for comments and suggestions.

Sasha Romanosky
RAND Corporation, sromanos@rand.org

Richard Sharp
Microsoft, rsharp@gmail.com

Alessandro Acquisti
Heinz College, Carnegie Mellon University, acquisti@andrew.cmu.edu

1. Introduction

Firms have many options for investing in security technologies in order to protect their corporate databases and intellectual property from cyberattack or improper disclosure. Indeed, the worldwide market for IT security tools reached over $60 billion dollars in 2013 (Gartner 2013), and the US Government alone spent approximately $65 billion on security controls from 2006-2013 (Coburn 2014). However, conditional on these ex ante investments, data breaches still occur and impose massive costs. A recent 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). Indeed, TJMax suffered costs over $250 million due to a breach in 2007 (TJX 2007), and Heartland Payment Systems spent $150 million in legal fees and fines from its breach of 100 million credit cards in 2007 (Yadron 2014). In some of these cases consumers bear substantial harms themselves to various forms of financial and medical identity theft. For example, there were approximately 16.6 million household victims of identity theft in 2012 (which is in part attributable to data breaches), with total (direct and indirect) losses of $24.7 billion (Harrell 2014).

As a result of these breaches and the costs 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 (Maurushat 2009). By notifying consumers of the breach, the hope is that firms will invest in sufficient security controls to prevent a breach (Majoras 2005). A further consequence of the publicity from public disclosure is that firms bear 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 an event 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 costs ex post. On the other hand, if breaches are rare and relatively low magnitude, it may be cheaper to mitigate the cost ex ante. Indeed, this tension was raised during a 2005 discussion by Gartner who 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."[1] And a popular security research firm found that survey respondents felt 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).

But the firm's investments are not borne in isolation. Consumer behavior (and therefore consumer losses) are affected by a firm's actions, and certainly policy makers have an 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

[1] *Id.*

for protecting digital assets (NIST 2014). Applying the economic analysis of accident law to an information technology problem, we investigate the strategic decision by firms when investing in ex ante versus ex post security controls. We model firm costs by considering the consequence of recent data breach disclosure laws, consumer liability, and the firm's impact on consumer behavior and overall social welfare. Specifically, we address two questions: how should firms manage ex ante security precautions with ex post breach efforts following a data breach?; Under which conditions can a social planner minimize social costs.

2. Background

Our research contributes to the Information Systems (IS) literature, and in particular to the streams of studies on the economics of information security, and specifically research related to optimal investment and information disclosure. From a methodological perspective, our research leverages the microeconomic literature on accident law.

The body of IS literature related to information security has grown considerably in recent years, and some attention in this field has been paid to optimal investment in security and the disclosure of breaches, vulnerabilities, and software bugs (Cavusoglu et al. 2008, Telang and Wattal 2007, Gandal et al. 2009, Grossklags et al. 2008). Numerous 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 et al. 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 strong 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) that examines 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. Overall, they find that investment should be less than one-third of the expected loss from a breach. Note, however, that this work 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, 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.

In summary, despite the prevalence of security technologies available to firms, data breaches still occur and are costly. The trade-offs they face, therefore, is understanding how to balance ex ante prevention investments with ex post mitigation efforts. 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 private litigation. In addition, some of the theoretical IS literature has examined optimal investment in security patching and software vulnerability, even though the empirical literature has (just) started investigating the impact of *data breach*. However, no analytical research has yet examined the costs and consequences of data breaches in regard to ex ante prevention and ex post mitigation activities, which is our focus.

Moreover, our approach differs from traditional models involving externalities in four important 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). Therefore, we extend traditional accident models by explicitly incorporating the consumer's cost of mitigating actions. Third, we extend typical accident models to specifically account for both ex ante, and ex post care. Finally, we proceed beyond typical modeling procedures which directly account for firm or consumer activity, and model social costs at consumer and firm equilibrium levels (that is, *evaluated at agents' privately optimal levels of care*).

Therefore, to our knowledge, this article is the first to theoretically analyze firm, consumer, and social 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, compromising the personal information of its customers. In many cases once the firm learns of the breach, it will be required to notify affected individuals.[2] The reasons are threefold. First, 47 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 in an effort 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.[3]

Once consumers are informed of the breach by the firm, they become empowered to take action in order to reduce any identity theft. But the firm's responsibilities are not over. Once it 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 care.[4] 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,

[2] Certainly before a firm can notify individuals it must become aware of the breach. This may occur in a number of 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 the purpose of our analysis, however, the method by which the firm learns of the breach does not drive disclosure, and is therefore not considered.

[3] 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 the purpose of 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.

[4] 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 in order to refer to activities taken by the firm to either prevent a breach or reduce the cost from a breach.

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, the firm 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.[5] 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 remediate any damage, and it can offer credit monitoring or identity theft insurance to affected individuals.[6] We denote the magnitude of this reputation loss as $r(x_2) \geq 0$ which we assume is decreasing and convex in x_2.[7] Of course, all of these ex post investments come at a cost, and so we denote the cost these activities as $d(x_2) \geq 0$ which is increasing and convex in x_2, continuous and twice differentiable.

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 in an attempt to recover any losses (Romanosky and Acquisti 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 none. 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 $\alpha H_{ID}(x_2, y)$.[8]

[5] See also (Hoffman 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).

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

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

[8] 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).

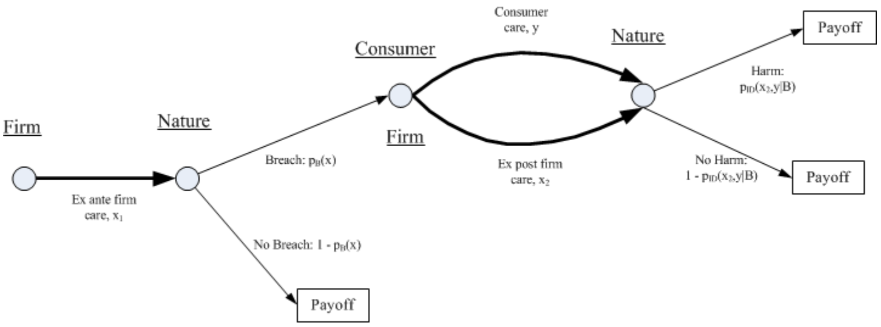

Figure 1 **Sequence of events**

3.2. Consumer costs

We described 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, $h_{TE} \geq 0$.

First, 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 $0 \leq p_{ID}(x_2, y) \leq 1$.[9] For brevity however, we do not distinguish between the probability or magnitude of harm but 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 2-player, combined sequential and simultaneous 2-period game (we do not include Nature in the count of the players).

In the first period the firm determines its optimal level of ex ante breach prevention, x_1, after which Nature determines with probability $p_B(x_1)$ whether or not a breach will occur. Then, in the

[9] Practically speaking, 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. This could easily be accounted for by including an additional parameter, $0 < p_0 < 1$ to our model. However, given that by definition it is independent of firm or consumer action, it would not qualitatively affect our results, and so we omit it for brevity.

second period the firm and consumer jointly 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 care to minimize her losses from identity theft. Finally, Nature determines with probability $p_{ID}(x_2, y|B)$ whether the consumer will suffer identity theft, $h_{ID}(x_2, y)$.[10] As is commonly done, we solve this game using backward induction by first solving for the simultaneous consumer and ex post firm levels of care, then solving for the firm's optimal level of ex ante care (which is a function of x_1, x_2, and y).

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

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

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

$$C(x_2, y) = p_B(x_1)\,(h_{TE}(y) + (1 - \alpha)\; H_{ID}(x_2, y)) \tag{2}$$

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

$$S(x_1, x_2, y) = c(x_1) + p_B(x_1)\,(i + d(x_2) + r(x_2) + \; H_{ID}(x_2, y) + h_{TE}(y)) \tag{3}$$

3.4. Equilibrium solutions

3.4.1. Generalizable form There exists a unique solution (a pure strategy Nash equilibrium) to the generalizable two-player game described in the equations above.

Proof Proofs for the existence and uniqueness of solutions are given in Ozdaglar (2010). Existence follows from recognizing that the scenario is a continuous, 2-player game with bounded strategy sets (user and firm activity is non-negative and, for practical purposes, finite). This is an application of Glicksberg's theorem (Ozdaglar 2010, slide 4). Uniqueness then follows due to the convexity of the strategy sets and cost functions (Ozdaglar 2010, slide 26). Note that this proof is not constructive, so to find the solution we apply backward induction. First, the 2-player simultaneous game in which the firm and consumer determine the values of x_2 and y is solved. It is a system of two equations in two unknowns: the derivative with respect to x_2 of Eq. 1 set equal to zero and the derivative of Eq.

[10] Note that we implicitly consider that a data breach and the fraudulent use of consumer data are 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.

2 with respect to y set equal to zero. One may note that x_1 actually drops out of these equations, which demonstrates that 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 are left with a convex optimization problem in x_1 defined by the derivative of Eq. 1 with respect to x_1 set equal to zero.[11] □

Since neither the firm nor the consumer bears the full cost of their actions, we know that neither will engage in the socially optimal level of care. We therefore 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 social costs.

3.4.2. Specific form While we have shown a pure strategy Nash equilibrium solution to the generalizable cost functions, we next illustrate the solutions for specif functional (quadratic) forms. Let the cost and probability functions be defined as follows

$$\begin{aligned} c(x_1) &= \gamma x_1^2 \\ p_b(x_1) &= \frac{1}{(1+\phi x_1)^2} \\ d(x_2) &= \delta x_2^2 \\ r(x_2) &= \frac{\rho}{(1+\sigma x_2)^2} \\ h_T(y) &= \eta y^2 \\ H(x_2,y) &= \frac{\theta}{(1+\mu x_2)^2(1+\nu y)^2} \end{aligned}$$

To find the equilibrium solution, we first find the simultaneous solution for the ex post mitigation efforts by solving the following system of equations,

$$\left.\frac{\partial F}{\partial x_2}\right|_{(\tilde{x}_2,\tilde{y})} = 0$$
$$\left.\frac{\partial C}{\partial y}\right|_{(\tilde{x}_2,\tilde{y})} = 0$$

Note that $\tilde{x}_2$ and $\tilde{y}$ do not depend on x_1 in which case we obtain a pair of optimal values rather than expressions for the optimal values in terms of x_1. First, we solve the second equation for y in terms of x_2.

$$p_b(x_1)\left(2\eta y + (1-\alpha)\frac{-2\theta\nu}{(1+\mu x_2)^2(1+\nu y)}\right) = 0$$

[11] In some cases, it may be difficult to solve the (x_2, y) system algebraically, however, one may applied a numerical method based on fixed point iteration that quickly converges to the solution in practice.

$$\begin{aligned}
\eta y\left(1+\nu y\right)-\left(1-\alpha\right)\frac{\theta\nu}{\left(1+\mu x_2\right)^2} &= 0\\
\eta\nu y^2+\eta y-\left(1-\alpha\right)\frac{\theta\nu}{\left(1+\mu x_2\right)^2} &= 0
\end{aligned}$$

By noting that $y\geq 0$, we therefore have

$$\tilde{y}=\frac{1}{2\eta}\left(-1+\sqrt{1+\frac{4(1-\alpha)\theta\nu^2}{\eta\left(1+\mu\tilde{x}_2\right)^2}}\right)$$

We now substitute this expression into the equation $\left.\frac{\partial F}{\partial x_2}\right|_{(\tilde{x}_2,\tilde{y})}=0$ in order to find the value of $\tilde{x}_2$

$$\begin{aligned}
p_b(x_1)\left(2\delta x_2-2\frac{\rho\sigma}{1+\sigma x_2}-2\alpha\frac{\theta\mu}{(1+\mu x_2)(1+\nu y)^2}\right) &= 0\\
\delta x_2-\frac{\rho\sigma}{1+\sigma x_2}-\alpha\frac{\theta\mu}{(1+\mu x_2)(1+\nu y)^2} &= 0\\
\delta x_2-\frac{\rho\sigma}{1+\sigma x_2}-\alpha\frac{\theta\mu}{(1+\mu x_2)\left(1+\nu\frac{1}{2\eta}\left(-1+\sqrt{1+\frac{4(1-\alpha)\theta\nu^2}{\eta(1+\mu x_2)^2}}\right)\right)^2} &= 0\\
\left(1+\mu x_2\right)\left(\delta x_2-\frac{\rho\sigma}{1+\sigma x_2}\right)\left(1+\frac{\nu}{2\eta}\left(-1+\sqrt{1+\frac{4(1-\alpha)\theta\nu^2}{\eta\left(1+\mu x_2\right)^2}}\right)\right)^2-\alpha\theta\mu &= 0
\end{aligned}$$

The equilibrium value for x_2 is defined implicitly by this last equation,

$$\left(1+\mu\tilde{x}_2\right)\left(\delta\tilde{x}_2-\frac{\rho\sigma}{1+\sigma\tilde{x}_2}\right)\left(1+\frac{\nu}{2\eta}\left(-1+\sqrt{1+\frac{4(1-\alpha)\theta\nu^2}{\eta\left(1+\mu\tilde{x}_2\right)^2}}\right)\right)^2-\alpha\theta\mu=0$$

With the values of $\tilde{x}_2$ and $\tilde{y}$ in hand, we turn to $\tilde{x}_1$, which must satisfy the following equation,

$$\begin{aligned}
\left.\frac{\partial F}{\partial x_1}\right|_{(\tilde{x}_1,\tilde{x}_2,\tilde{y})} &= 0\\
2\gamma x_1-\frac{2\phi}{1+\phi x_1}\left(i+\delta\tilde{x}_2^2+\frac{\rho}{(1+\sigma\tilde{x}_2)^2}+\alpha\frac{\theta}{(1+\mu\tilde{x}_2)^2(1+\nu\tilde{y})^2}\right) &= 0\\
2\gamma x_1-\frac{2\phi}{1+\phi x_1}\Gamma(\tilde{x}_2,\tilde{y}) &= 0\\
\gamma x_1(1+\phi x_1)-\phi\Gamma(\tilde{x}_2,\tilde{y}) &= 0\\
\gamma\phi x_1^2+\gamma x_1-\phi\Gamma(\tilde{x}_2,\tilde{y}) &= 0
\end{aligned}$$

and again noting that $x_1\geq 0$ we have,

$$\tilde{x}_1=\frac{-\frac{1}{2}+\sqrt{\frac{1}{4}+\frac{\phi^2\Gamma(\tilde{x}_2,\tilde{y})}{\gamma}}}{\phi}$$

Now that we have achieved formal expressions for the firm and consumer cost equations, we next examine firm behavior.

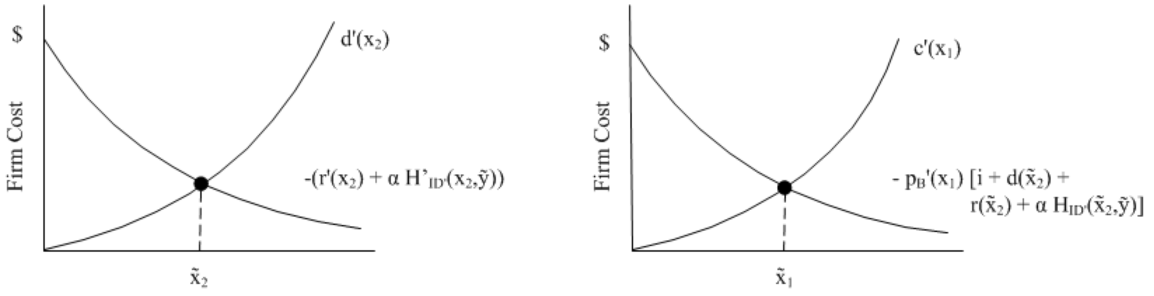

Figure 2 Two optimization problems

4. Firm Behavior

4.1. What drives firm costs and behavior?

Because we are interested in both firm costs and behavior before and after data breach, we examine how firm costs, and ex ante and ex post activities are driven by the components of Equation 1.

Notice from Equation 1 that absent the public disclosure of a breach,[12] 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, $d(x_2)$, and 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, $p_B(x_1)(.)$.

Efforts taken by firms to reduce the effects of a data breach are affected by a number of 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 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 cheaper costs of disclosure would increase mitigation efforts, it would reduce total breach costs.

Proposition 1. *As the cost of notifying consumers becomes cheaper, firms will take more effort to mitigate breach losses, and total firm costs will decrease.*

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, 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

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

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 an increasing number of data breach lawsuits, or as settlement awards dried up.[13] And consumer identity theft would decline as consumers, themselves, begun to take more action to reduce their losses.

PROPOSITION 2. *As reputational or consumer harms decrease, firms will take less effort to mitigate breach losses, but total firm costs will decrease.*

The amount of security investment taken ex ante, x_1, is affected by a number of 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.*

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.*

As described above, an increase in ex post breach costs (disclosure, reputation, or consumer redress) will increase expected losses from a data breach, driving up prevention efforts, illustrating how ex ante prevention is affected by ex post losses (or illustrating how breach *prevention* is driven by breach *mitigation*). However, the opposite is not true. The amount of mitigation activities 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 is irrelevant.

PROPOSITION 5. *While ex ante prevention controls are a function of ex post mitigation activities, ex post mitigation is independent of any ex ante costs.*

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

5. Social welfare analysis

In the previous sections, we examined the costs imposed on firms and consumers as a result of a data breach. We now examine the effect of changes in these costs on aggregate social cost at equilibrium.

What factors drive social cost?

Changes in firm and consumer costs will have two very different and non-obvious effects on social welfare. For example, when a particular 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 social costs will be affected in an entirely different manner.

As discussed, firms may bear substantial settlement costs as a result of a data breach lawsuit, and Romanosky et al. (2012) 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). Second 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 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 right panel of Figure 3, 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 is driven to invest more closely to the socially optimal level of care ($\tilde{x}_B > \tilde{x}_A$).[14] Notice that this is achieved without change to the social cost function. On the other hand, 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 in the left panel of Figure 3.[15] 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.

We now examine the conditions under which social costs can be minimized. We again emphasize that the 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).

[14] This occurs because the change in α represents a transfer of cost between the firm and consumer. As mentioned, when $\alpha = 0$, the consumer bears all damages from identity theft (the firm bears none), and when $\alpha = 1$, 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.

[15] 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).

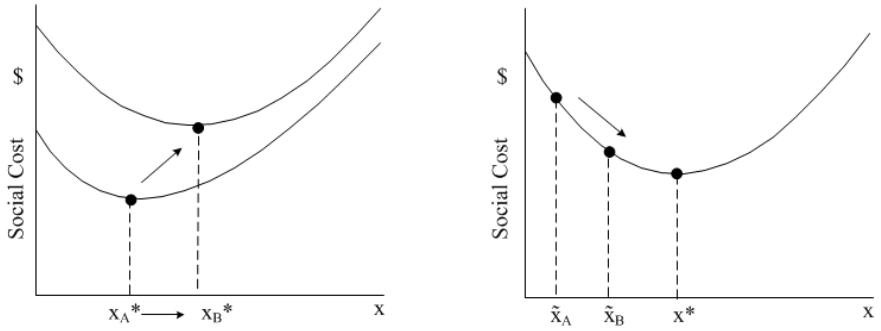

Figure 3 Movement of, and along, the social cost curve

How can consumer liability minimize social costs?

The extent to which a firm should bear more or less consumer harm is currently under 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" (Schwarzenegger 2007). At first, one may assume that social costs are minimized when the firm internalizes all consumer loss (i.e. as $\alpha \to 1$). 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 avoid the accident and eliminate the externality).[16] Because our situation involves a continuum of prevention activities, we must therefore employ more rigorous analytical solutions.

We are able to show that there is an optimal value of liability, $0 < \alpha^* < 1$, 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 α when $\alpha = 0$ and decreasing α when $\alpha = 1$, but there must be a value α^* within this interval at which $\partial S/\partial\alpha = 0$:

[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.

PROPOSITION 6. *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* $\partial S / \partial \alpha |_{\alpha = \alpha^*} = 0$.

6. Computational analysis

We support the propositions of this paper by illustrating the behavior of the firm's ex ante prevention and ex post mitigation activities with a computational simulation as shown in Figure 4. While robust to other convex functional forms, the following discussion applies only to the this class of functions. Figure 4 was produced from the following class of quadratic expressions: $c(x_1) = x^2$, $p_B(x_1) = 1/(1 + x_1^2)$, $d(x_2) = x_2^2$, $r(x_2) = 10/(1 + x_2^2)$, $H_{ID}(x_2) = 1/(1 + x_2^2 + y^2)$, $h_{TE}(y) = y^2$, $i = 15$, $\alpha = 0.5$, with values chosen for illustrative purposes only. The global minimum is also shown as a point in the $x_1 - x_2$ plane of Figure 4.

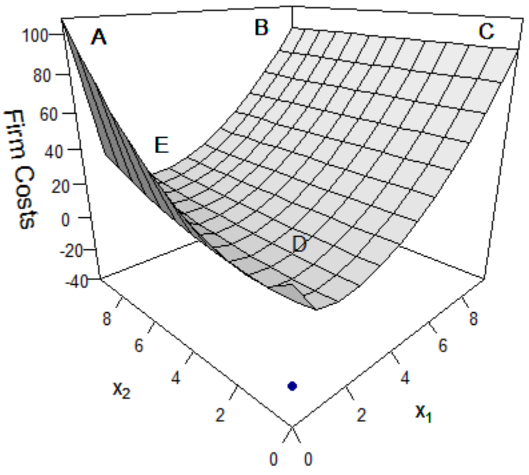

Figure 4 **Graphical representation of firm costs**

We first illustrate the contributions of the firm's cost function that govern each of the areas labeled.

Region A is affected primarily by the costs of breach breach investigation, i, and disclosure, $d(x_2)$. In this area of low prevention and high mitigation activities, the cost of prevention is minimal, whereas the probability of breach approaches 1. High mitigation efforts drive reputation and consumer losses toward zero, leaving only the costs of disclosure and investigation. i.e. $F(\sim 0, x_2) = \sim i + d(x_2)$. Regions B and C are dominated by the cost of prevention controls (x_1) regardless of the level of mitigating activities (x_2) by the firm because at very high levels of prevention the probability of a breach approaches zero, diminishing the effects of any ex post costs associated with a breach. i.e.

$F(x_1) = \sim c(x_1)$. In region D near the origin, firm costs approach $i + r(0) + \alpha * H_{ID}(y)$, suggesting that for extremely low levels of breach prevention and mitigation activities, firm costs are driven mainly by the cost of breach investigation, the reputation harm absent any mitigating efforts by the firm, and the portion of consumer harm borne by the firm. Finally, region E is generated from a modest amount of prevention controls, x_1, and shows how firm costs are largely inelastic to changes in mitigation controls, x_2 (region D-E). However, notice how (for this class of quadratic functions), firm costs are very sensitive to changes in ex ante prevention.

Next, observe that in general, the correlation between ex ante prevention (x_1) and ex post mitigation (x_2) activities is positive, causing firm costs to decrease (or increase) in both x_1 and x_2 together. For instance, in regions A and B (at high and low values of x_1 and high values of x_2), the firm would rationally choose to reduce both prevention and mitigation efforts. However, this behavior is not universal. There are regions in which the marginal benefit from investing in prevention (x_1) is much larger than the marginal benefit from investing in mitigation (x_2). For example, at very high levels of prevention (regions B to C), the marginal reduction in firm costs is much greater from reduced prevention than from reduced mitigation, regardless of the level of mitigation.

But this behavior changes at low levels of prevention (region D). At relatively low levels of both prevention and mitigation, the marginal reduction in overall cost is small for both prevention and mitigation efforts. Further, for intermediate levels of prevention (region D to E), depending on the amount of mitigation, increasing investments in mitigation may have opposing effects. Region E shows how firm costs are increasing in either more or less prevention, while region D shows decreasing costs with less prevention.

In order to quantify these observations further, we provide some empirical estimates of these factors in the following section.

7. Empirical estimates

While robust data is difficult to obtain, some information regarding overall security spending, and data breach costs are available.

First, overall spending on information security technologies was estimated to be around \$60 billion globally in 2012, and expected to approach \$86 billion in 2016 (Infosec 2012). A study from 2013 found that a an average firm's IT budget was around 5% of its revenues (CIO 2013). For a firm with \$2 billion in sales (a medium to large enterprise), this would represent an IT budget of \$100 million annually. Further, a Gartner survey of 1500 firms in 2010 found that firms spend an average of 5% of their IT budget on information security (Kirk 2010), suggesting that an average firm might spend only \$5 million annually on information security controls .[17]

[17] This is likely an underestimate of the magnitude spent to secure an organization's network given the positive externalities enjoyed by other forms of IT infrastructure that also help to protect a corporate network.

Information regarding the probability of a breach has been estimated in ongoing unpublished work by this author. In this research, we find that the probability of any given firm suffering a data breach is less than 1%, with retail, IT and financial companies suffering proportionally greater breach rates.

In regard to overall data breach costs, NetDiligence examined cost data from about 60 cyber insurance claims and found an average of total losses of $3.7 million (Greisiger 2012). In addition, the Ponemon Institute has been conducting annual surveys of data breach costs since 2005 and provides one of the most comprehensive analyses available. While the survey data reflect only a small sample of firms, additional inferences can be gained from the time trends of these data. First, the most recent study estimates the average total cost of a data breach $5.4 million per breach (Ponemon 2013).

Of this $5.4 million total, the data suggest that the cost of breach investigation and analysis, i, comprises around $0.4 million, or around 7.4% of total costs. Further, it finds that overall disclosure costs (which include notification costs, customer support activities legal fees, etc), $d(x_2)$, comprise almost $2 million, or 36.5% of the total cost. Note that included in this figure would be consumer losses internalized by the firm. Finally, the survey results find that reputation losses, $r(x_2)$, due to lost business, customer churn, and loss of goodwill account for over $3 million, or 56% of all overall costs (and in fact, this proportion has decreased in recent years from a high of $4.5m in 2010). If correct, this suggests that reputation harms account for a considerable (indeed, larger than half) proportion of a firm's data breach losses – an impressive and sobering amount. In addition, the study finds that certain industries such as transportation, healthcare and communications suffer about a 50% larger cost-per-record loss (around $300), while retail and hospitality industries suffer a far lower cost-per-record amount of around $100.

Separate estimates for consumer losses from all forms of identity theft range from about 0-$300 for median losses and $422-$675 for mean losses.[18] These estimates refer to out of pocket expenses and do not include the dollar equivalent of time and effort spent addressing the crime, nor other forms of social cost (which may include higher insurance premiums, increased interest rates, civil legal actions, and so forth (Baum 2004). Since these costs represent the loss from all types of identity theft, we must scale it by the portion of identity theft due to data breaches, $p_{ID}(x_2)$. Javelin Strategy and Research (2006), claims that "businesses as a source of information breach account for 30% of cases," while in a later study they find that only 11% of identity theft is caused by data breaches

[18] The available data is quite sparse, but some estimates are available: $0 (Federal Trade Commission (2007), Table 2, median loss of all forms of identity theft; Javelin Strategy and Research (2006), p. 2, median loss), $500 (Federal Trade Commission (2003), Table 2, average loss of all forms of identity theft), $555 (2003), $675 (2005), $422 (2006) (Javelin Strategy and Research (2006), p. 2, average loss), $300 (Baum (2005), Table 7, median loss).

(Javelin Strategy and Research 2009, Fig. 2). Another study finds using data from the US Secret Service that about 26% of identity theft cases are due to data breaches (Gordon et al. 2007). By averaging these values, a rough approximation suggests that data breaches represent about 20% of identity theft, resulting in a range of median losses between \$84-\$135 per consumer. For a breach affecting 100k consumers, this would represent consumer losses, and an estimate of $H_{ID}(x_2, y)$, between \$8.4m and \$13.5m.

We can also provide some estimate of the amount of consumer loss internalized by the firm and, therefore, the magnitude of α. First, if we use the median consumer loss of \$0 reported by Federal Trade Commission (2007) (Table 2) and by Javelin Strategy and Research 2006 (p. 2), we would automatically find $\alpha = 1$. However, the losses may be underestimated, as they do not account for the consumer time and effort involved in addressing identity theft. If we consider mean (not median) data published by Javelin Strategy and Research (2006) (p. 2), out-of-pocket consumer expenses were \$555 (2003), \$675 (2005), \$422 (2006), and total amounts stolen were \$5,249 (2003), \$5,885 (2005) and \$6,383 (2006). Imputing a 20% portion of loss to data breaches, we obtain $\alpha = 0.47$ (2003), $\alpha = 0.43$ (2005), and $\alpha = 0.67$ (2006), respectively, which suggests that firm do bears a substantial portion of consumer loss.

8. Discussion

Now that we have constructed a data breach accident model, we can examine how different policy interventions might affect these outcomes. For example, a policy maker might ask – and firm would certainly be concerned with the question of: *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 (Pigou 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.

Now, importantly, this approach suffers from two important issues: the amount of consumer harm actually caused by the breach (fraud, privacy invasion, increased interest rates, etc) is largely unknown, often unquantifiable, and small in magnitude. In general, it is very difficult for consumers to fully and rationally compute the harm caused by data breaches. Moreover, because of the nature of identity theft, victims are often unable to uniquely identify the particular firm or breach which led to the harm. Together, these characteristics suggest that, in absence of 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.

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?* The minimal social cost is achieved when both the firm and consumer each bear some portion of consumer harm. Therefore, social costs would not be minimized whenever only one party bears the full cost. This is due to the fact 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.

From the discussion above, and under the caveat of the limited set of data currently available in this field, data breaches are costly, and impose a significant burden on firms. This suggests that 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 the majority of 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.

References

Acquisti, A., A. Friedman, R. Telang. 2006. Is there a cost to privacy breaches? An event study. *Fifth Workshop on the Economics of Information Security.*

BakerHostetler. 2014. Bakerhostetler data breach chart. *BakerHostetler Data Breach Chart* URL `http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf`.

Barth, J., J. Cordes. 1980. Optimal financial disclosure with and without SEC regulation. *Quarterly Review of Economics and Business* **20**.

Baum, K. 2004. *Identity Theft, 2004*. Bureau of Justice Statistics.

Baum, K. 2005. *Identity Theft, 2005*. Bureau of Justice Statistics.

Brodkin, J. 2007. Choicepoint settles with 43 states over data breach. *Network World* URL `http://www.networkworld.com/news/2007/053107-choicepoint-settles-data-breach.html`.

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

Cavusoglu, H., H. Cavusoglu, H. Zhang. 2008. Security patch management: Share the burden or share the damage? *Management Science* **54**(4) 657–670.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2004. 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* **9**(1).

CIO. 2013. 2013 state of the cio. *CIO Magazine* URL `http://www.cio.com/documents/pdfs/2013%20State%20of%20the%20CIO%20Exec%20Summary.pdf`.

Coburn, Tom. 2014. 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* URL `http://www.coburn.senate.gov/public/index.cfm?a=Files.Serve&File_id=f1d97a51-aca9-499f-a516-28eb872748c0`.

Federal Trade Commission. 2003. *2006 Identity Theft Survey Report*. Federal Trade Commission.

Federal Trade Commission. 2007. *2006 Identity Theft Survey Report*. Federal Trade Commission.

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

Gandal, N., J. Choi, C. Fershtman. 2009. Network security: Vulnerabilities and disclosure policy. *Journal of Industrial Economics* Forthcoming.

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

Gartner. 2013. Gartner says worldwide security market to grow 8.7 percent in 2013. *Gartner Inc* URL `http://www.gartner.com/newsroom/id/2512215`.

Gordon, G., J. Rebovich, K. Choo, J. Gordon. 2007. Identity fraud trends and patterns: Building a data-based foundation for proactive enforcement. *Center for Identity Management and Information Protection* Utica College.

Gordon, L. A., P. L. Martin, W. Lucyshyn, , T. Sohail. 2006. The impact of the Sarbanes-Oxley act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy* **25**(5) 503–530.

Gordon, Lawrence A., Martin P. Loeb. 2002. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.* **5**(4) 438–457.

Greisiger, M. 2012. Cyber liability and data breach insurance claims. *NetDiligence* URL `http://www.netdiligence.com/files/CyberClaimsStudy-2012sh.pdf`.

Grossklags, J., N. Christin, J. Chuang. 2008. Secure or insure? A game-theoretic analysis of information security games. *In Proceedings of the 17th International World Wide Web Conference, Beijing, China* 209–218.

Harrell, E. 2014. Victims of identity theft, 2012. *Bureau of Justice Statistics, U.S. Department of Justice* URL `http://www.bjs.gov/content/pub/pdf/vit12.pdf`.

Hoffman, C., C. Shih. 2014. What is expedient notification of a "data breach? *Mondaq Business Briefing* URL `http://http://www.mondaq.com/unitedstates/x/294034/data+protection/What+is+Expedient+Notification+of+a+Data+Breach`.

Hogan, Lovells. 2014. Data breaches: Time for high alert, avoiding and managing the legal risks of cybersecurity incidents. *Hogan and Lovells* URL `http://www.hldataprotection.com/2014/03/articles/cybersecurity-data-breaches/upcoming-hogan-lovells-webcast-will-address-data-breach-preparedness-and-response/`.

Infosec. 2012. Global security spending to hit 86b in 2016. *InfoSecurity Magazine* URL `http://http://www.infosecurity-magazine.com/view/28219/global-security-spending-to-hit-86b-in-2016/`.

Javelin Strategy and Research. 2006. Identity fraud survey report Consumer Version.

Javelin Strategy and Research. 2009. Identity fraud survey report Consumer Version.

Jin, G., P. Leslie. 2003. The effect of information on product quality: Evidence from restaurant hygiene grade cards. *Quarterly Journal of Economics* **118**(2) 409–451.

Kannan, K., J. Rees, S. Sridhar. 2007. Market reactions to information security breach announcements. *International Journal of Electronic Commerce* **12**(1) 69–91.

Kaplan, D. 2010. Heartland settles with discover over breach. *SC Magazine* URL `http://www.scmagazine.com/heartland-settles-with-discover-over-breach/article/178116/`.

Kingston, M. 2014. 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* URL `http://www.judiciary.senate.gov/imo/media/doc/02-04-14KingstonTestimony.pdf`.

Kirk, J. 2010. How much should you spend on it security? *Computerworld* URL `http://www.computerworld.com/s/article/9187239/How_much_should_you_spend_on_IT_security_`.

Kolstad, C., T. Ulen, G. Johnson. 1990. Ex post liability for harm vs. ex ante safety regulation: Substitutes or complements? *American Economic Review, American Economic Association* **80**(4) 888–901.

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

Lemos, R. 2009. Tjx estimates breach costs at $118 million. *Security Focus* URL `http://www.securityfocus.com/brief/568`.

Majoras, D. 2005. 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 .

Maurushat, A. 2009. Data breach notification law across the world from California to Australia. *University of New South Wales Faculty of Law Research Series* URL `http://law.bepress.com/cgi/viewcontent.cgi?article=1153&context=unswwps`.

McGrath, M. 2014. Target profit falls 46on coming. *Forbes* 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/`.

Mulligan, J. 2014 URL `http://`.

NIST. 2014. Framework for improving critical infrastructure cybersecurity. *National Institute of Standards and Technology* URL `http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm`.

Orrick. 2014. Targeting harm from a breach: Plaintiffs lawyers get creative in data privacy suits. *Orrick, Herrington and Sutcliffe LLP.* 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`.

Ozdaglar, A. 2010. Game theory with engineering applications lecture 6: Continuous and discontinuous games. *MIT Course 6.254* 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`.

Pigou, Arthur C. 1932. *The Economics of Welfare*. Library of Economics and Liberty.

Ponemon. 2011. *2011 Annual Study: Cost of a Data Breach*. The Ponemon Institute.

Ponemon. 2013. 2013 cost of data breach study: Global analysis. *Ponemon Institute LLC* URL `http://`.

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

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

Romanosky, Hoffman D., S., A. Acquisti. 2014. Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies* **11**(1) 74–104.

Romanosky, S., R. Telang, A. Acquisti. 2011. Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management* **30**(2) 256–286.

Schwarzenegger, A. 2007. Letter to the members of the California state assembly URL `http://gov.ca.gov/pdf/press/2007bills/AB%20779%20Veto%20Message.pdf`.

Shavell, S. 1984. A model of the optimal use of liability and safety regulation. *The RAND Journal of Economics* **15**(2) 271–280.

Telang, R., S. Wattal. 2007. An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering paper* **33**(8) 544–557.

TJX. 2007. The tjx companies, inc. reports strong second quarter fy08 operating results, estimates liability from computer systems intrusion(s). *Press Release TJX Companies* URL `http://investor.tjx.com/phoenix.zhtml?c=118215&p=irol-newsArticle&ID=1040186&highlight=`.

Trustwave. 2014. Trustwave global security report 2013. *Trustwave* URL `http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf`.

Verrecchia, R. 2001. Essays on disclosure. *Journal of Accounting and Economics* **32**(1) 97–180.

Wang, T., J. Rees, K. Kannan. 2009. The impact of information security disclosures on market reactions to security breaches. Under review.

Westervelt, R. 2014. Investment in data breach responders lacking, study finds. *CRN Online* URL `http://www.crn.com/news/security/300071737/investment-in-data-breach-responders-lacking-study-finds.htm`.

Wolf, F. 2011. Recent case opens the door for data breach class actions. *Kroll Cyber Security Blog* URL `http://www.krollfraudsolutionsblog.com/2011/11/recent-case-opens-the-door-for-data-breach-class-actions/`.

Yadron, D. 2014. Companies wrestle with the cost of cybersecurity. *The Wall Street Journal* URL `http://online.wsj.com/news/articles/SB10001424052702304834704579403421539734550`.

9. Appendix A

9.1. Tables

A summary of variables used in the model is shown in Table 1, and a summary of the equations representing expected firm, consumer, and aggregate costs both is shown in Table 2.

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 1 Variables

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	$c(x_1)+p_B(x_1)\,(i+d(x_2)+r(x_2)+\;H_{ID}(x_2,y)+h_{TE}(y))$

Table 2 Firm, consumer, and social cost function