Policy Framework for Data Breaches

Rahul Telang | Carnegie Mellon University

Data breaches and firms' responses to them have been in the headlines for the past few years. They seem as inevitable as death and taxes. The recent massive breach at JP Morgan—a bank with high security standards—is a worrisome continuation of the trend. Although some breaches are widely covered in newspapers, many occur at small firms that get little attention. To put it in perspective, according to Privacy Clearinghouse (www.privacyrights.org), more than 4,400 data breaches have been recorded in the US since 2005, exposing nearly one billion records.

Why are we seeing so many breaches? Why aren't firms protecting their data more aggressively? And, what can we do about it?

These questions aren't new. California passed the data breach notification law in 2003. However, it seems that, in the US, neither firms nor policymakers have made much progress. Therefore, it's a good time to revisit some economic and policy fundamentals of data breaches. My goal here is to offer a broad framework to highlight various tradeoffs and the intuition behind them.

Firm Losses versus Customer Losses

Data breaches hurt users—their information is stolen and they become victims of financial fraud and identity theft. In many cases, victims have little recourse to recover their losses. Firms often are also hurt, potentially incurring some cost in identifying and cleaning up breaches.

Suppose a firm invests money in security, such as new technology, employee training, or policy formulation. Despite these investments, a breach might still occur, causing customer losses $h(s)$, where s is the security investment. Thus, $h(s)$ should be interpreted as customer losses conditional on breach. Investment s can affect both the probability of a breach and the magnitude of loss.

$h(.)$ is a function of s such that more security investment by a firm will reduce breach possibility and hence reduce $h(.)$. So customer loss is a decreasing function of the firm's security investment. Firms might also incur losses after a breach, or $f(s)$. As with $h(.)$, $f(.)$ is a decreasing function of s: more security investment would reduce firm loss.

The expected cost of breaches to the society, which economists call social cost S, is the sum of user cost $h(s)$ and firm cost $f(s) + s$, that is, $S = h(s) + f(s) + s$. To minimize the total social cost S, a socially optimal security investment s^* is necessary; however, this typically won't eliminate breaches completely—a point to which I will return.

Firms might not fully internalize customer losses and thus might not minimize the same social cost function S. Let's say a firm internalizes only a fraction λ of user losses. The firm's private cost is $C = \lambda\, h(s) + f(s) + s$. An optimizing firm would minimize C. Because $0 < \lambda < 1$, that firm would choose a security level $\acute{s}$ less than s^*. In other words, the firm invests less than we'd like owing to the externality of data breaches—data breaches cause customer loss that the firm won't fully compensate absent some regulations.

The smaller the λ, the lower the firm's investment and the larger the gap between what we want the firm to do versus what the firm would do if left alone. The value of λ varies depending on market structure, industry type, the number of dominant players, and so on. Obviously, this representation doesn't include all complexities, but it captures the essential tradeoffs quite well.

How Can Policymakers Get Firms to Do More?

Policymakers regulate firms in two broad ways—ex-post and ex-ante regulations. (For a more technical discussion, see Steven M. Shavell's "A Model of the Optimal Use of Liability and Safety Regulation."[1])

Ex-Post Regulations

Ex-post regulations, such as penalties, taxes, and liability payments,

Copublished by the IEEE Computer and Reliability Societies

occur after an adverse event has taken place. (In this article, I don't distinguish between administrative regulations and legal rules.) For example, policymakers might introduce regulations such that after a data breach, firms are held liable for customer losses or pay a penalty for the breaches. This penalty should be enough to force firms to internalize customer losses. If imposed with certainty, a penalty of $(1 - \lambda)h(.)$ makes $C = S$. Thus, the firm would take the same precautions and investments that a policymaker would.

The US Federal Trade Commission has—and sometimes exercises—the authority to penalize firms for data breaches.[2] For example, some regulations require firms to provide free credit monitoring to customers after a breach. However, penalties or other services required of firms might not be large enough to offset potential customer losses.

A stricter form of ex-post regulation would be to hold firms directly liable for consumer harm. For instance, recent proposed amendments in California disclosure law would hold retailers directly liable for customer losses.[3] Unfortunately, many frauds and thefts due to data breaches generally occur later, making it difficult to prove attribution and connect a customer's loss to a particular data breach. Court costs and uncertainty of outcomes also act as significant deterrent. These frictions can make liability laws less effective in getting firms to invest optimally.

The US relies on transparency and disclosures to encourage firms in competitive markets to invest more in security. The lynchpin is the data breach notification laws. After California SB 1386 passed in 2003, 47 states passed a law requiring firms to send breach notices to users. So, even though it's ex-post regulation in spirit, the penalty is for not disclosing the breach. The notification laws don't hold the firm directly liable for customer losses.

There are two levers to these notification laws. First, the notification should alert consumers to take preventive steps that might help them reduce losses. For example, banks might issue replacement credit and debit cards.[4] Second, the notifications should inform consumers about poor security practices to allow them to make better choices. Thus, the laws and associated media scrutiny acts like sunlight that can disinfect. The goal is to get firms to internalize more of their customer losses via increased competition and fear of a bad reputation.

Pull quote for departments: Approximately 20-25 words. Pull quote for departments: Approximately 20-25 words. Pull quote for departments: Approximately 20-25 words.

The Security and Exchange Commission has taken similar efforts to provide guidelines on how and when corporations should disclose data breach risks and cyberattacks in their public filings for investors. A widespread criticism of these laws is that firms must comply with each state law separately, as each state has a different definition of what constitutes a breach as well as different notification deadlines. This adds significant compliance cost. One widely discussed alternative is a uniform nationwide notification law, which would prevent heterogeneous statues. It remains to be seen if such a bill could go through Congress.

Despite these laws being on the books, little empirical evidence supports or disputes disclosure laws' effectiveness.[5] We don't know if firms' compliance cost outweighs user benefits or what important tweaks are necessary to make these laws more cost-effective. Solid empirical research on data breach laws is sorely needed for effective policymaking.

Ex-Ante Regulations

Ex-ante regulations bite firms before adverse events occur, requiring firms to comply with certain business and technology standards. For instance, retailers must comply with Payment Card Industry (PCI) Data Security Standards, proposed by the major credit card networks. Retailers are audited and penalized for noncompliance. Compliance must occur whether or not the firm has had a breach. Note that the PCI standard is a proposed self-regulation rather than a government mandate.

The Gramm-Leach-Bliley (GLB) Act and the Fair Credit Reporting Act (FCRA) are other examples. GLB specifies data security requirements for nonbank financial institutions, and FCRA requires consumer reporting agencies to use reasonable procedures to ensure that entities have a permissible purpose to receive sensitive consumer information. It also imposes safe disposal obligations.

Thus the ex-ante regulations make firms invest directly in security protections. In practice, the regulatory landscape is complex, and a combination of both ex-post and ex-ante laws push firms to invest more in data protection. Without policy intervention, firms wouldn't invest in the socially optimal amount of security. The goal is to impose a combination of ex-ante and ex-post costs that induce firms to invest as close to s^* as possible.

Investing in security is expensive, and at some point, the incremental reduction in breach costs will be less than the incremental cost of additional security. Thus, the

occurrence of a data breach generally isn't sufficient evidence that a firm underinvested in security. Of course, customers still would incur costs and might have little or no recourse unless the firm is directly held liable. But, in the long run, a robust insurance market should overcome this problem. After an optimal investment, whatever remains is a residual risk that should be spread via insurance firms, just as in any other market. However, whether a robust insurance market can emerge remains to be seen.

Information Sharing

Another type of regulation entails a more explicit government role. Wise security investments by firms can deter breaches and lower potential losses. However, as I discussed, even firms investing the socially optimal amount in security won't eliminate all breaches. But some government actions—taken in concert with optimal firm investments—could further reduce breaches.

Suppose I add a function $\delta(v)$ to the social cost function $S^+ = \delta(v)[f(s) + \lambda h(s) + s]$. The function $0 < \delta(v) < 1$ represents a reduction in social cost induced by a government investment of v. For example, v might include efforts to trace and punish hackers. If hackers are deterred by such efforts, breach attempts will decrease. Similar to λ, $\delta(v)$ differs from industry to industry and is an empirical question. Note that reducing the cost of breaches lowers the socially optimal firm investment s^*.

In addition, data breaches are highly technical, and firms might not know for a while that they were breached. Suppose a data- and intelligence-sharing mechanism let breached firms effectively share data with other firms or trusted government agencies. With earlier detection, a breach might be rendered less costly or prevented from spreading to other firms.

Unfortunately, getting firms to share sensitive information with government agencies or with one another is very challenging. During the Clinton administration, many industry information sharing and analysis centers were established with the explicit goal of data sharing. However, there's little systematic and transparent analysis to suggest that they're effective.

Firms need incentive to share useful information. Some legislative proposals recommend ways to make it attractive for private firms to share sensitive security breach data with government agencies.[6] Two important features of these bills are a mechanism letting firms report anonymously and protection against lawsuits. Whether such a bill would pass and how effective it would it be remain to be seen.

Thus far, the US policy to improve security and privacy has focused on disclosure and transparency. However, consumers must be willing to suitably punish firms for lax security behavior. Current policymaking rests on many assumptions and conjectures. To update our policy framework, we need more and better studies evaluating which policy levers work and which don't for us.

Better security will come at a cost. If we as a society want better security, we should to be willing to pay for it. ■

Rahul Telang is a professor of information systems and management at the Heinz College, Carnegie Mellon University. Contact him at rtelang@andrew.cmu.edu.

References

1. S.M. Shavell, "A Model of the Optimal Use of Liability and Safety Regulation," *Rand J. Economics*, vol. 15, no. 2, 1984, pp. 271–280.
2. G. Stevens, "The Federal Trade Commission's Regulation of Data Security under Its Unfair or Deceptive Acts or Practices (UDAP) Authority," Congressional Research Service, 11 Sept. 2014; http://fas.org/sgp/crs/misc/R43723.pdf.
3. K. Lerner, "Calif. Bill Would Make Retailers Liable in Data Breaches," Law 360, 7 Apr. 2014; www.law360.com/articles/525774.
4. P. Rosenblum, "Home Depot Data Breach: Banks' Response Is Critical to Consumer Reaction," *Forbes*, 19 Sept. 2014; www.forbes.com/sites/paularosenblum/2014/09/19/home-depot-data-breach-banks-response-is-critical-to-consumer-reaction.
5. S. Romanosky, R. Telang, and A. Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?," *J. Policy Analysis and Management*, vol. 30, no. 2, 2011, pp. 256–286.
6. R. King, "Senate Intelligence Committee Approves Cybersecurity Sharing Bill," ZDnet, 8 July 2014; www.zdnet.com/senate-intelligence-committee-approves-cybersecurity-sharing-bill-7000031368.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.