Cybercriminals pose a growing threat to corporate and personal information. Although governments have focused on the problem of information security for decades, rising dependence on digital data both for personal and corporate use has led to an increase in opportunities for cybercriminals to benefit from illegal access to that data. High-profile data-loss incidents at Honda, NASDAQ, Sony, Target, RSA Security, Lockheed Martin as well as warnings from several national governments about data security have heightened concerns in the private sector. An ongoing discussion in information security is the tension between the role of government to ensure the safety of its citizens versus the ability of the market to achieve efficient solutions on its own [4]. Recognizing that the risk posed by data loss is multifaceted, this study digs deeper into the relationship between data loss incidents and stock price impact by analyzing data breach announcements from the years 2000 to 2012 for publicly traded corporations listed on the New York stock and NASDAQ stock exchanges.

This article helps make sense of the appropriate role of government by checking to see if the markets are incentivizing good information security policies. This research builds on other studies that have looked at the stock-price impact, but expands the data set used across market sectors, which will help confirm the validity of the previous research. In addition, this research looks for differences across various breach types to help provide guidance to decision makers on prioritizing information security investments.

Given corporate vulnerability to costly breaches, information security has moved “up the chain” with the establishment of C-level information security officer position in many firms. The creation of the CISO position reflects the reality that, in the words of a senior executive, “we are all IT companies” and there are significant risks associated with that reality [18]. Cybercriminals, attracted by low risk and high rewards, target information through a variety of means that range from taking advantage of software vulnerabilities to social engineering. Regardless of the attack vector, however, the outcome is the same: sensitive corporate and personal information end up in the hands of malicious actors. The recognition of cybercrime can be seen through the increasing popularity of insurance to transfer the risk [16] and the superior performance of information security stocks that have outperformed the market since 2011 [23].

By Kristopher Dane – ISSA member, Puget Sound Chapter

This article discusses the threat of cybercrime and data breaches to organizations. The author discusses the economics of data breach information and then reviews the existing public data on breaches to see how markets are responding. The article concludes with a call to action to normalize breach reporting to better inform consumers and enable future research.
The persistent threat of cybercrime and the various attack methods won’t be new to the readers of this journal, but what might be new are the ways in which public policy can help address aspects of the data-breach problem. Before we dive into the analysis, let’s first take a step back and consider the role of public policy. Jonathan Gruber’s text, *Public Finance and Public Policy*, [10] outlines key questions that are relevant to the role of government in the economy:

1. When should government intervene in the economy?
2. How might the government intervene?

Generally, governments intervene in the economy for two reasons: to achieve efficiency (ensuring optimal production) or to achieve equity (ensuring a desired distribution of resources throughout the society). When markets are not achieving efficient outcomes, governments can step in to correct the failure. There are many potential causes of market failure, but here the focus is on one particular cause: imperfect information.

An important element of a competitive market is information flow. In order to have a truly competitive market, both the buyer and the seller must have information on anything that would impact their decision-making process. Researchers Roberds and Schreft describe the market for consumer information by describing a person’s confidentiality as an economic good whose provision depends on two other goods:

1. The amount of personally identifiable information (PII) incorporated into that person’s transactional identity
2. The level of security for this data or the degree of data integrity [20]

As more information about a consumer is included in his or her transactional identity, it becomes easier for payment processors to reduce account fraud. At the same time, however, increasing the amount of PII collected about consumers reduces their privacy and increases the impact if the data is misused. While consumers can be informed of the amount of PII incorporated into their transactional identity by reading the privacy statements, they cannot access information on security of their data.

**How secure is my data?**

While corporations in some sectors are required to outline anticipated uses for consumer data in privacy statements, there is no such requirement for disclosing the security measures that protect customer data. In 2003, California was the first to enact a data breach notification law. California Senate Bill 1386 requires notification if PII is “reasonably believed to have been acquired by an unauthorized person” [5]. Now almost every state has a similar law requiring consumer notification when PII has been lost or stolen. While this is a good start, the definition of what constitutes PII or what constitutes a breach vary widely from state to state and consumers don’t know what is done to prevent future breaches. Whereas laws such as Sarbanes-Oxley require audits of financial records via third-party auditors and statements to the Securities and Exchange Commission, there is no consistent standard for information security.

The legislation and regulations defining information security standards have largely been sector specific:
• The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that certain healthcare-related information be secured.

• The 1999 Gramm-Leach-Bliley Act (GLBA) applies to the financial sector and requires financial institutions to develop an information security program.

• The 2002 Federal Trade Commission (FTC) Standards for Safeguarding Customer Information (Safeguards Rule) requires financial institutions under FTC jurisdiction to secure customer data.

• Federal Financial Institutions Examination Council (FFIEC) has a working group that monitors cybersecurity and provides tools to member organizations to assess their risk exposure [8].

• The 2002 Federal Information Security Management Act (FISMA) applies to government agencies and contractors and requires that an information security management strategy be set up consistent with NIST guidelines (NIST 800-53).

• Payment Card Industry Data Security Standard (PCI DSS) applies to organizations that handle credit cards by ensuring that merchants meet prescriptive security guidelines according to their transaction volume. Validation of compliance is performed annually, either by an external qualified security assessor or by self-assessment questionnaire.

A commonly cited market failure is that of information asymmetry, where one party to a transaction has much more information than the other. An information asymmetry currently exists between firms and between firms and consumers regarding data breaches [13]. If a firm is breached but does not release the information to the public, the consumer is potentially damaged by identity theft. The piecemeal approach to regulating information security can leave certain sectors unregulated and, even for the regulated industries, consumers may not know what regulatory agency applies to a particular company without significant research. Furthermore, companies that are not covered by existing regulation may still hold corporate intellectual property or sensitive information on employees that should be secured to protect the company, the employee, and the competitiveness of our national economy. Enacting regulation that requires minimum standards with public notification of audits could raise awareness of information security and risk management across all sectors. In the words of Bruce Schneier, “Regulation—SOX, HIPAA, GLB, the credit-card industry’s PCI, the various disclosure laws, the European Data Protection Act, whatever—has been the best stick the industry has found to beat companies over the head with. And it works. Regulation forces companies to take security more seriously, and sells more products and services” [21].

The absence of publicly available security and breach information places investors at a disadvantage when it comes to assessing the risk position of a firm. Indeed, the absence of this information also affects anyone who is doing research into data breaches, including this author. Datalossdb.org, an organization affiliated with the Open Security Foundation that relied on volunteers to transcribe data breach announcements in order to maintain an open source database, stopped making their database available for download during the period this research was being conducted. Their website now refers to a private company called Risk Based Solutions that provides access to their data for a fee and provides some analysis of that data in periodic reports. If this information is not freely available for people who are looking for it, how can we expect consumers to make decisions based on it?

**Does information matter?**

In light of these potential challenges to the efficient functioning of the market, scholars from a variety of disciplines have begun to explore the impact of data on companies. Subramani and Walden looked at the impact of e-commerce announcements on stock price [22]. Others have studied the impact of data-breach announcements on the stock price of corporations [9][2] and at the longer term financial performance of breached companies, finding negative impact in both cases [14]. Telang and Wattal found a 0.6% loss in the stock price of software vendors following a vulnerability report [24]. Including firm size along with the data-breach characteristics explains some of the cross-sectional variation in stock price [6]. Research has also taught us that the prevalence of cybercrime is based on an economic calculation of

---

1 In the interest of full disclosure, I should say that I have not requested access to the data from Risk Based Solutions. It is entirely possible that they would provide the complete data set, but the point here is that the information should be public and easy to access.
availability of hacking skills relative to economic opportunity, and critically the attacker’s selection of target is based on not only symbolic significance but also weakness in defense mechanisms [15]. Research has also shown that hackers are rational actors, and those who are more rational engage in preparation and reconnaissance, and their attacks are more successful than their more impulsive counterparts [3].

Now that we know that clear information is important in a market and that hackers are rational actors responding to the information available to them, we need to look to see if consumers and investors are responding to information on breaches. Previous research tells us that we should expect to see a small negative impact on stock price. This research significantly expands the sample size of data breaches and draws on a random sampling of data breaches for analysis rather than pre-selecting market sectors. Additionally, this study breaks up the data breaches into breach types, allowing us to examine if the market is punishing companies more or less depending on the nature of the breach.

Preparing for analysis

There are many ways in which a corporation can lose data and several classification schemata exist. Here we have adopted the classification schema developed by security experts Matthew Curtin and Lee Ayers [7], who split data breaches into three main categories:

- **Physical breaches**: There is a loss of physical control over the data. Physical losses are characterized by the loss of documents, computers, and media such as compact discs, tapes, and other drives.

- **Logical breaches**: There has been a failure of the information security management system. This is where the controls in place were exploited by employees (insider threat) or outsiders (hacker). These breaches occur due to “loop-holes” in the security systems that are in place where the corporation’s information security controls have failed.

- **Procedural breaches**: The corporation mishandled the data. These breaches are characterized by the loss of data through mailings, a.k.a. “snail mail,” publicly accessible information on the corporate website, or improper disposal of records.

We may expect investors to be more forgiving of a novel attack that causes a data breach over a breach caused by accidentally mailing PII out to customers.

Data breach incident data was downloaded from the data loss incident database at datalossdb.org. The data included information on 5005 incidents that were narrowed down to 1023 incidents by eliminating incomplete records and those outside range of available stock-price information. The datalossdb data used a different breach classification schema than that used in this analysis, so the data was translated from the 25 category schema provided to the three breach category schema. Tables 1 and 2 show the final incident count in each category as well as the mapping between the datalossdb breach types and the types used in this analysis.

Data Breach Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>388</td>
</tr>
<tr>
<td>Logical</td>
<td>499</td>
</tr>
<tr>
<td>Procedural</td>
<td>136</td>
</tr>
</tbody>
</table>

Table 1 – Re-Categorized incident counts

2 Datalossdb.org previously provided a tool that allowed for the complete database to be downloaded as a csv file but this is no longer the case. The data for this study was downloaded without headers from http://datalossdb.org/exports/dataloss.csv on 2/26/2012. Similar data may be accessed through other sources such as Privacy Rights Clearing House.
The analysis

This research looks for differences between the data-breach incidents as they are separated into different groupings. Several statistical tests were run to look for results with "statistical significance." These tests look for differences in the data that are unlikely to be caused by chance.4 "Statistical significance" does not necessarily mean practical significance, which is why it is important to carefully consider the questions being asked to be sure the answers are actually useful. The data that we have allows us to ask several questions. In order to help inform the development of government regulation, we will assess the extent to which the market is self-regulating information security by asking the following questions:

- Do breached companies suffer a negative stock-price impact?
- Is the degree of the stock-price impact correlated with the number of records lost?
- Do more recent breaches show a greater stock-price impact?

Then we will try to guide information security investments by checking to see if there are differences across data-breach types by asking the following questions:

- Does the stock-price impact differ across breach types?
- Does the number of records lost differ across breach types?

---

3 Due to licensing agreements, the author may not release the completed data used in this study as it includes pay-for-access data.

4 This is quite a simplification and I recommend that those interested do some additional research, especially since data-driven decision making can be powerful and statistical tools are widely available (Microsoft Excel Analysis ToolPak, the open source R software). A free textbook can be found here: [https://www.openintro.org/stat/textbook.php](https://www.openintro.org/stat/textbook.php) or the following courses can introduce you to the basics: [https://www.coursera.org/course/stats1](https://www.coursera.org/course/stats1); [https://www.khanacademy.org/math/probability](https://www.khanacademy.org/math/probability).
Finally, considering the growing awareness of security and the enactment of legislation and corporate policies to address the problem, we will ask:

- Is the number of records lost dropping over time?

The data-breach incident data, combined with the stock-price data, was loaded into an SQL database. A random sample was taken from each breach type for analysis and the stock-price impact was calculated using the following equations:

\[
\text{Stock Price Impact} = \frac{\% \text{ Stock Price Change} - \% \text{ Index Price Change}}{% \text{ Stock Price Change} - % \text{ Index Price Change}}
\]

<table>
<thead>
<tr>
<th>Negative stock-price impact but breach size doesn't matter?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Do breached companies suffer a negative stock-price impact?</strong></td>
</tr>
<tr>
<td>Yes, a stock-price impact of -0.65% was found.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Is the degree of the stock-price impact correlated with the number of records lost?</th>
</tr>
</thead>
<tbody>
<tr>
<td>No correlation was found.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Do more recent breaches show a greater stock-price impact?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unclear, a statistically significant difference was detected between the time periods, but the trend is inconsistent.</td>
</tr>
</tbody>
</table>

This analysis shows that there is a statistically significant difference between the mean index-price change and the mean stock-price change in the data set. This difference is consistent with previous research; however, it is small at -0.65% and differs from the sometimes cataclysmic calls that a data breach will crash the stock of a company. To be sure, there are significant costs associated with a breach including notification and identity-protection provision, but the drastic stock-price drop isn’t apparent in the data.

From the perspective of aligning market punishment with loss of public information, it is troubling that no correlation was found between stock-price impact and the number of records lost. This indicates that the market is not aware of or simply not responding to differing scales of information loss. Additionally, while the data is unclear, the stock-price impact shown over the three time periods (table 4) is trending in the wrong direction if you expect consumers to be punishing companies that suffer breaches. There is some evidence to suggest that consumers are tiring of breach announcements and not changing their behavior after a breach as they accept it as a cost of doing business [1]. This data may be a reflection of that trend.

### Stock-Price Impact Over Time

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Mean Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 5, 2001 - December 31, 2006</td>
<td>0.35%</td>
</tr>
<tr>
<td>January 1, 2007 - December 31, 2008</td>
<td>-1.88%</td>
</tr>
<tr>
<td>January 1, 2009 - January 26, 2012</td>
<td>0.22%</td>
</tr>
</tbody>
</table>

Table 4 – Mean stock-price impact over time

### Does the stock-price impact differ across breach types?

Yes, a statistically significant difference was found between the logical breach type and the procedural breach type with mean impacts of -2.32% and 0.728% respectively.

### Does the number of records lost differ across breach types?

Yes, a statistically significant difference in the number of records lost was found between the physical and procedural breach categories. The complete results are shown in the tables.

<table>
<thead>
<tr>
<th>Is the number of records lost per incident dropping over time?</th>
</tr>
</thead>
</table>
| No, the data was split into three date ranges, and the analysis did not show a statistically significant difference between the three ranges.

The significant stock-price impact found between the logical and procedural breach types with respective means of -2.32% and 0.728% remind us that there is noise in the data caused by other factors influencing stock price (since it would seem strange that a data breach of any type may result in a bump in stock price). The negative impact as a result of the logical breaches may be an indication that the market is becoming aware of the need for robust information security management systems and is punishing companies that implement those systems poorly.

This awareness of the logical breaches may be due to the significant number of records lost due to this type of breach. While the statistically significant difference was found between the physical and procedural breaches, the logical breaches show a mean loss of 6.4 million records per incident. As mentioned above, the lack of statistical significance between the logical and other breaches means that we can’t rule out these results being chance, but applying professional judgment, we know major losses are possible.

### Records Lost Across Breach Types

<table>
<thead>
<tr>
<th>Breach Type</th>
<th>Mean Records Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>449,294</td>
</tr>
<tr>
<td>Logical</td>
<td>6,411,905</td>
</tr>
<tr>
<td>Procedural</td>
<td>96,660</td>
</tr>
</tbody>
</table>

Table 5 – Records lost across breach types
When considering public and corporate investments to limit the amount of information being lost, this analysis provides direction. The logical breaches may be a good place to start to limit the magnitude of the loss. Secondly, this analysis shows that physical data breaches result in significantly more records being lost at a mean of 449,294 records per incident, whereas procedural breaches result in a mean of 96,660 records lost per incident. With an increasingly mobile workforce it may be difficult to legislate that companies stop losing physical assets to theft or loss, but there may be an opportunity to mitigate the risk of record loss by limiting the number of records kept on mobile hardware. Finally, the analysis of records lost over time shows that the controls put in place over the past decade to control information loss may be having an impact. The mean number of records lost per incident has dropped from 2.4 million to 173,000 (table 6). If this drop makes you suspicious, it should. The difference isn’t statistically significant, which may mean that the drop is a result of chance. Further analysis with updated information may result in a better understanding of the drop over time.

#### Records Lost Over Time

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Mean Records Lost</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 5, 2001 - December 31, 2006</td>
<td>2,427,383</td>
</tr>
<tr>
<td>January 1, 2007 - December 31, 2009</td>
<td>2,509,727</td>
</tr>
<tr>
<td>January 1, 2010 - January 26, 2012</td>
<td>172,938</td>
</tr>
</tbody>
</table>

Table 6 – Records lost over time

### Conclusion and a call to action

Considering that the data-breach notification laws are now in place in almost every state and data-breach announcements are becoming daily events, this study might yield different results if repeated. Some reports indicate that the year 2015 set a record for the number of data-breach reports, which could be an indication that the notification laws are working to add information to the market [19].

We discussed the importance of clear and available information if the market is to self-regulate and the potential for the government to help fill the gaps if necessary. This analysis has shown that the market does respond to data breach announcements although the impact is small. Government efforts to enact data-breach notification legislation has taken a step toward leveling the information asymmetry between consumers and companies because some information on breaches is now available, but more needs to be done because we have seen that the market isn’t responding to breaches based on the records lost. We have also seen that there would be a benefit to repeating this type of research with updated information to measure the effectiveness of data-breach announcement laws or the impact of security-awareness efforts. The challenge, however, is that there is no publicly available, standardized database of data-breach incidents, nor do consumers have a measure of the security of their data.

As professionals who could benefit from impartial analyses and from the exchange of accurate information regarding data breaches, we should be pushing:

- Major industry players or government bodies to fund the creation of an accepted clearinghouse of breach information along the lines of the Common Vulnerabilities and Exposures database [17] that can be accessed by any interested party and is consistently available and free of charge. This would allow for consistent impartial analysis from a variety of fields that can continue to guide our internal investments in security. This data source should also be made readable for the general public so they can become informed about risks to their personal information [11].

- Normalization of state level data breach notification regulations so that companies can spend more time addressing the core security concerns and less time navigating the various compliance regimes that they face from state to state while maintaining a “high bar” for protection [12]. This normalization should include standardizing the definition of PII, notification triggers, notification time frames, and may also require notification when vectors for access to PII such as stolen online credentials are compromised. These credentials may be reused across accounts and compromise can “result in access to all, including banking and otherwise supposedly secure accounts” [11].

- Development of a forum to discussion what security audits (along the lines of the financial audits required for publicly traded companies) might consist of. These audits would provide information to consumers and business partners on the maturity of the information security management strategies in place and would allow for companies to choose business partners who don’t increase their risk exposure. Finally, these audits would allow investors to accurately place information security risk alongside other risks as they make their investment decisions.

All of these measures would help ensure consistent and available information is available in the marketplace, which will help regulators, investors, and information security professionals monitor the success and impact of information security investments.

### Bibliography

Do Data Breaches Matter? A Review of Breach Data and What to Do Next | Kristopher Dane


About the Author

Kristopher Dane, Associate at the international engineering firm Thornton Tomasetti, Inc., is a graduate of the University of Washington (UW) Master of Arts in Policy Studies program and a graduate of the Information Assurance and Risk Management Certificate Program at University of Washington. Kris holds certifications from the Department of Defense Committee on National Security Systems and is a member of the Evergreen State chapter of Infragard. He previously spent nine years as a Technical Program Manager before joining Thornton Tomasetti, where he brings his analytical, programming, and modeling skills to serve their Structural and Protective Design Practices. Kris may be reached at kristopherdane@gmail.com.