Does a Data Breach Harm Industry Peers? Evidence from the U.S. Retail Industry

September 9, 2021

Jaeyoung Park

Postdoctoral researcher, Yonsei University
Data Breaches


Source: https://blog.auditanalytics.com/ranking-the-equifax-data-breach-updated/
Investors’ Perspective

- Most investors consider **cybersecurity** to be a critical component of risk oversight and they are engaging with portfolio companies to better understand how cybersecurity risk is governed and managed.

- A considerable body of research have explored **how investors react to security issues (events)**.
  - **Information security investment** leads to 1.36 percent increase of abnormal returns for firms (Chai et al, 2011); **ISO 27001 certification announcements** are associated with positive abnormal market value creation (Deane et al., 2019).
  - **Data privacy breach announcement** negatively affects the market value of the firm in general, although the negative impact is different across industries and type of breaches (Acquisti, et al., 2006; Malhotra & Malhotra 2011; Tripathi & Mukhopadhyay, 2020).

- Although previous research has demonstrated how a data breach can generate negative consequences to **the breached firm**, there is a lack of understanding of how a data breach at one firm affects **other firms** that have not been breached.

**Guilt by association (“contagion effect”) vs. Gain by misfortune (“competition effect”)**
Conceptual Framework of a Data Breach Spillover

Data breach

- Visibility of data breach risk

Similarity

Investors’ perceptions

Market value of other firms
Information transfers are said to occur if announcements (events) made by one group of firms contemporaneously affect the returns of another group of non-announcing firms (Schipper, 1990). e.g., bankruptcy (Lang & Stulz, 1992), accounting restatements (Gleason et al., 2008), financial misconduct (Paruchuri & Misangyi, 2015), or even environmental problems (Barnett & King, 2008).

This effect can occur if information released by a firm has important implications for the future profitability of other non-announcing competitors.

The information transfer effect typically arises among intra-industry firms rather than among completely unrelated companies, and it exists when information released by one firm affects the performance of other non-announcing competitors in the same industry (Szewczyk, 1992; Guo, 2017)

There were negative mean abnormal returns among Internet firms that were not attacked: the competitors were presumed to be in a similar situation to the announcing firm owing to industry commonalities (Ettredge & Richardson, 2003).
Theoretical Background: Cybersecurity Risk Disclosure

The SEC issued a disclosure guidance regarding cybersecurity in 2011.

- According to the guidance, public companies should disclose the risks of cyberattacks or security breaches in their SEC filings if such incidents “are among the most significant factors that make an investment in the company speculative or risky” (SEC, 2011).

- Cybersecurity risk disclosure provides investors with useful information about firms’ cybersecurity risks, and it may be positively associated with the market valuation.

---

Division of Corporation Finance
Securities and Exchange Commission

CF Disclosure Guidance: Topic No. 2
Cybersecurity

Date: October 13, 2011

Summary: This guidance provides the Division of Corporation Finance’s views regarding disclosure obligations relating to cybersecurity risks and cyber incidents.

Supplementary Information: The statements in this CF Disclosure Guidance represent the views of the Division of Corporation Finance. This guidance is not a rule, regulation, or statement of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved its content.
# TABLE OF CONTENTS

## PART I
- **Item 1** Business
- **Item 1A** Risk Factors
- **Item 1B** Unresolved Staff Comments
- **Item 2** Properties
- **Item 3** Legal Proceedings
- **Item 4** Mine Safety Disclosures
- **Item 4A** Executive Officers

## PART II
- **Item 5** Market for the Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities
- **Item 6** Selected Financial Data
- **Item 7** Management's Discussion and Analysis of Financial Condition and Results of Operations
- **Item 7A** Quantitative and Qualitative Disclosures About Market Risk
- **Item 8** Financial Statements and Supplementary Data
- **Item 9** Changes in and Disagreements with Accountants on Accounting and Financial Disclosure
- **Item 9A** Controls and Procedures
- **Item 9B** Other Information

## PART III
- **Item 10** Directors, Executive Officers and Corporate Governance
- **Item 11** Executive Compensation
- **Item 12** Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters
- **Item 13** Certain Relationships and Related Transactions, and Director Independence
- **Item 14** Principal Accountant Fees and Services

## PART IV
- **Item 15** Exhibits, Financial Statement Schedules

## SIGNATURES
**Competitive and Reputational Risks**

*Our continued success is dependent on positive perceptions of Target which, if eroded, could adversely affect our business and our relationships with our guests and team members.*

We believe that one of the reasons …

---

**Information Security, Cybersecurity, and Data Privacy Risks**

*If our efforts to provide information security, cybersecurity, and data privacy are unsuccessful or if we are unable to meet increasingly demanding regulatory requirements, we may face additional costly government enforcement actions and private litigation, and our reputation and results of operations could suffer.*

We regularly receive and store information about our guests, team members, vendors, and other third parties. We have programs in place to detect, contain, and respond to data security incidents. However, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently and may be difficult to detect for long periods of time, we may be unable to anticipate these techniques or implement adequate preventive measures. In addition, hardware, software, or applications we develop or procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise information security, cybersecurity, and data privacy. Unauthorized parties may also attempt to gain access to our systems or facilities, or those of third parties with whom we do business, through fraud, trickery, or other forms of deceiving our team members, contractors, and vendors.

---

**Legal, Regulatory, Global and Other External Risks**

*The COVID-19 pandemic has affected our business in many different ways, and may continue to amplify the risks and uncertainties facing our business and their potential impact on our financial position, results of operations, and cash flows.*

The COVID-19 pandemic has …
Examples of Cybersecurity Risk in the 10-K

Subcaptions of “low visible data breach risk” (no “data or information” keyword)

**Bob Evans Farms:** “We rely heavily on information technology and any material failure, interruption, or **security breach** in our systems could adversely affect our business.”

**McDonald’s:** “Information technology system failures or interruptions or **breaches of network security** may interrupt our operations.”

Subcaptions of “high visible data breach risk” (“data or information” keyword)

**Barnes & Noble:** “The Company faces data security risks with respect to **personal information**.”

**Big Lots:** “If we are unable to secure **company, employee, and customer data**, our systems could be compromised, our reputation could be damaged, and we could be subject to penalties or lawsuits.”

- Data breaches related to **Point of Sale (POS)** in the U.S retail industry (SIC code 52-59), which allows us to test for the data breach risk contagion effect, because the POS system can be seen as a common vulnerability (risk) that almost all retail firms have.

- Data source: the LexisNexis database and data breach related databases such as Privacy Rights Clearinghouse (privacyrights.org)

### Table 1. List of Breached Firms

<table>
<thead>
<tr>
<th>Event date</th>
<th>Event Firms</th>
<th>SIC</th>
<th>Asset [m$]</th>
<th>Employee [m$]</th>
<th>Revenue [m$]</th>
<th>Market value [m$]</th>
</tr>
</thead>
<tbody>
<tr>
<td>20131219</td>
<td>Target</td>
<td>5331</td>
<td>48,163</td>
<td>361,000</td>
<td>73,301</td>
<td>38,982</td>
</tr>
<tr>
<td>20140305</td>
<td>Sally Beauty Holdings</td>
<td>5990</td>
<td>1,950</td>
<td>26,450</td>
<td>3,622</td>
<td>4,300</td>
</tr>
<tr>
<td>20140902</td>
<td>Home Depot</td>
<td>5211</td>
<td>40,518</td>
<td>365,000</td>
<td>78,812</td>
<td>106,053</td>
</tr>
<tr>
<td>20141021</td>
<td>Staples</td>
<td>5940</td>
<td>11,175</td>
<td>83,008</td>
<td>23,114</td>
<td>8,591</td>
</tr>
<tr>
<td>20150302</td>
<td>Natural Grocers by Vitamin Cottage</td>
<td>5411</td>
<td>189</td>
<td>2,346</td>
<td>520</td>
<td>366</td>
</tr>
<tr>
<td>20150504</td>
<td>Sally Beauty Holdings</td>
<td>5990</td>
<td>2,030</td>
<td>27,470</td>
<td>3,753</td>
<td>4,233</td>
</tr>
<tr>
<td>20150615</td>
<td>Fred's</td>
<td>5331</td>
<td>649</td>
<td>9,148</td>
<td>1,970</td>
<td>613</td>
</tr>
<tr>
<td>20160511</td>
<td>Wendys</td>
<td>5812</td>
<td>4,108</td>
<td>21,200</td>
<td>1,870</td>
<td>2,933</td>
</tr>
<tr>
<td>20160519</td>
<td>Noodles &amp; Company</td>
<td>5812</td>
<td>240</td>
<td>10,600</td>
<td>455</td>
<td>254</td>
</tr>
<tr>
<td>20170619</td>
<td>The Buckle</td>
<td>5651</td>
<td>580</td>
<td>8,600</td>
<td>974</td>
<td>1,028</td>
</tr>
</tbody>
</table>
Method: Sample (industry peers)

- Data source: COMPSTAT from WRDS
- All non-breached firms with the same two-digit SIC code as breached firms.
- Standard Industrial Classification (SIC) codes are four-digit numerical codes assigned by the U.S. government to business establishments to identify the primary business of the establishment. The first two-digit of the SIC code indicates the major industry group, a definition widely used in the previous studies (e.g., Wang and Wang, 2019).
- After excluding any observations with confounding events at the time of the data breach or missing variables, I ended up with 310 samples of non-breached firms.
Method: Event Study

- The event study can offer insights in contexts where it would be more difficult to utilize alternative metrics of performance (Sorescu et al., 2017).
- Assuming efficient information processing of the breach announcement, the event window ought to be as short as possible (McWilliams and Siegel 1997). **CAR (-1,1)** is used as our dependent variable.

![Event Study Diagram](image)

Test abnormal return of rival firms

The announcement of data breach by a focal firm
## Method: Definition of Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dependent variable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAR (-1,1)</td>
<td>The cumulative abnormal return for the industry peers in the three days surrounding the data breach event</td>
<td>Eventus from WRDS</td>
</tr>
<tr>
<td><strong>Independent variable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visible data breach risk</td>
<td>Dummy variable, equal to 1 if “data” or “information” keywords are included in the subcaptions related to security risks in Item 1A of 10-k filings at the end of the fiscal year before the data breach, o otherwise.</td>
<td>EDGAR</td>
</tr>
<tr>
<td>Similarity</td>
<td>Dummy variable, equal to 1 if the non-breached firm’s four-digit SIC code is the same as the breached firm, o otherwise. For example, when a breached firm is Target (SIC code 5331), Costco Wholesale (SIC code 5399) is coded as 0, and Walmart (SIC code 5331) is coded as 1.</td>
<td>Compustat from WRDS</td>
</tr>
<tr>
<td><strong>Control variable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prior performance</td>
<td>The ratio of net income to total assets (Compustat annual item: NI/AT)</td>
<td>Compustat from WRDS</td>
</tr>
<tr>
<td>Firm size</td>
<td>Natural log of total assets in millions (Compustat annual item: AT)</td>
<td>Compustat from WRDS</td>
</tr>
<tr>
<td>Growth</td>
<td>The ratio between the book and the market value of firm’s equity (Compustat annual item: CEQ/MKVALT)</td>
<td>Compustat from WRDS</td>
</tr>
<tr>
<td>Massive breach</td>
<td>Dummy variable, equal to 1 if non-breached firms is sample of the Target or Home Depot breach is, o otherwise.</td>
<td>PRC</td>
</tr>
<tr>
<td>Past breach</td>
<td>Dummy variable, equal to 1 if non-breached firms experience data breach(es) prior to the breach, o otherwise.</td>
<td>PRC</td>
</tr>
</tbody>
</table>
Results: Data Breach Risk Contagion Effect

- The CAAR for the 3-day event window (-1,1) was -0.68% and was statistically significant (p < 0.001).
  It suggests that a data breach is likely to decrease industry peers’ shareholder value.
- Evidence of the negative spillover effect of data breach or the data breach risk contagion effect

Table 3. Impact of Data Breach on Abnormal Stock Returns for Industry Peers

<table>
<thead>
<tr>
<th>Event window</th>
<th>SIC sample (N = 310)</th>
<th>CAAR (%)</th>
<th>Uncorrected Patell Z</th>
<th>Generalized Sign Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0, 0)</td>
<td>-0.42</td>
<td>-3.077**</td>
<td>-3.464***</td>
<td></td>
</tr>
<tr>
<td>(-1, 0)</td>
<td>-0.64</td>
<td>-3.705***</td>
<td>-3.805***</td>
<td></td>
</tr>
<tr>
<td>(-1, 1)</td>
<td>-0.68</td>
<td>-3.320***</td>
<td>-2.669**</td>
<td></td>
</tr>
<tr>
<td>(-1, 2)</td>
<td>-0.72</td>
<td>-2.844**</td>
<td>-2.555**</td>
<td></td>
</tr>
<tr>
<td>(0, 1)</td>
<td>-0.45</td>
<td>-2.536**</td>
<td>-3.578***</td>
<td></td>
</tr>
<tr>
<td>(0, 2)</td>
<td>-0.49</td>
<td>-2.035*</td>
<td>-1.874*</td>
<td></td>
</tr>
</tbody>
</table>

Note. The symbols †, *, **, and *** denote statistical significance at the 10, 5, 1, and 0.1% levels, respectively, using a generic one-tail test.
Results: The Role of Similarity

- The market values of industry peers with high similarity significantly decreased, while those of industry peers with low similarity did not.

- In an event window of (-1,1), for example, the CAAR of the former was -1.602% and it was statistically significant (p < .001), whereas the latter was 0.173% and it was not statistically significant.

- The differences between groups were statistically significant for various event windows.

Table 4. Comparison Between Industry Peers by Similarity

<table>
<thead>
<tr>
<th>Event window</th>
<th>Low similarity (N = 158)</th>
<th>High similarity (N = 152)</th>
<th>Difference test</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CAAR (%)</td>
<td>t-value</td>
<td>CAAR (%)</td>
</tr>
<tr>
<td>(-1, 0)</td>
<td>0.126</td>
<td>.313</td>
<td>-1.480</td>
</tr>
<tr>
<td>(0, 1)</td>
<td>0.160</td>
<td>.520</td>
<td>-1.077</td>
</tr>
<tr>
<td>(-1, 1)</td>
<td>0.173</td>
<td>.407</td>
<td>-1.602</td>
</tr>
</tbody>
</table>

Note. CARs are calculated using the market model. The symbols *** denote statistical significance at the 0.1% levels.
The market values of industry peers with high visible data breach risks significantly decreased, while those of industry peers with low visible data breach risks did not.

In an event window of (-1,1), for example, the CAAR of the former was -1.223% and it was statistically significant (p < .001), whereas the latter was 0.267% and it was not statistically significant.

The differences between groups were statistically significant for various event windows.

<table>
<thead>
<tr>
<th>Event window</th>
<th>Low visible data breach risks (N = 118)</th>
<th>High visible data breach risks (N = 187)</th>
<th>Difference test</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CAAR (%) t-value</td>
<td>CAAR (%) t-value</td>
<td></td>
</tr>
<tr>
<td>(-1, 0)</td>
<td>0.293 .580</td>
<td>-1.194 -4.881***</td>
<td>2.942**</td>
</tr>
<tr>
<td>(0, 1)</td>
<td>0.124 .329</td>
<td>-0.743 -3.237***</td>
<td>2.085*</td>
</tr>
<tr>
<td>(-1, 1)</td>
<td>0.267 .524</td>
<td>-1.223 -3.903***</td>
<td>2.638**</td>
</tr>
</tbody>
</table>

Note. CARs are calculated using the market model. The symbols *, **, and *** denote statistical significance at the 5, 1, and 0.1% levels.
Discussion

- One firm’s data breach harms the market value of industry peers.
  - This study provides additional evidence for the data breach risk contagion effect, indicating one firm’s loss is also its competitor’s loss.

- The data breach risk contagion effect is stronger for non-breached firms with high similarities to a breached firm, compared to those with low similarities.

- The data breach risk contagion effect is stronger when the risk of data breaches is visibly disclosed in industry peers’ 10-K report.
  - The market response to cybersecurity risk disclosures offers mixed results.
  - This study adds new evidence to the effect of cybersecurity risk disclosure.
Thank you for your attention.
Any questions or comments?