10th Asia Privacy Bridge Forum 2021

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

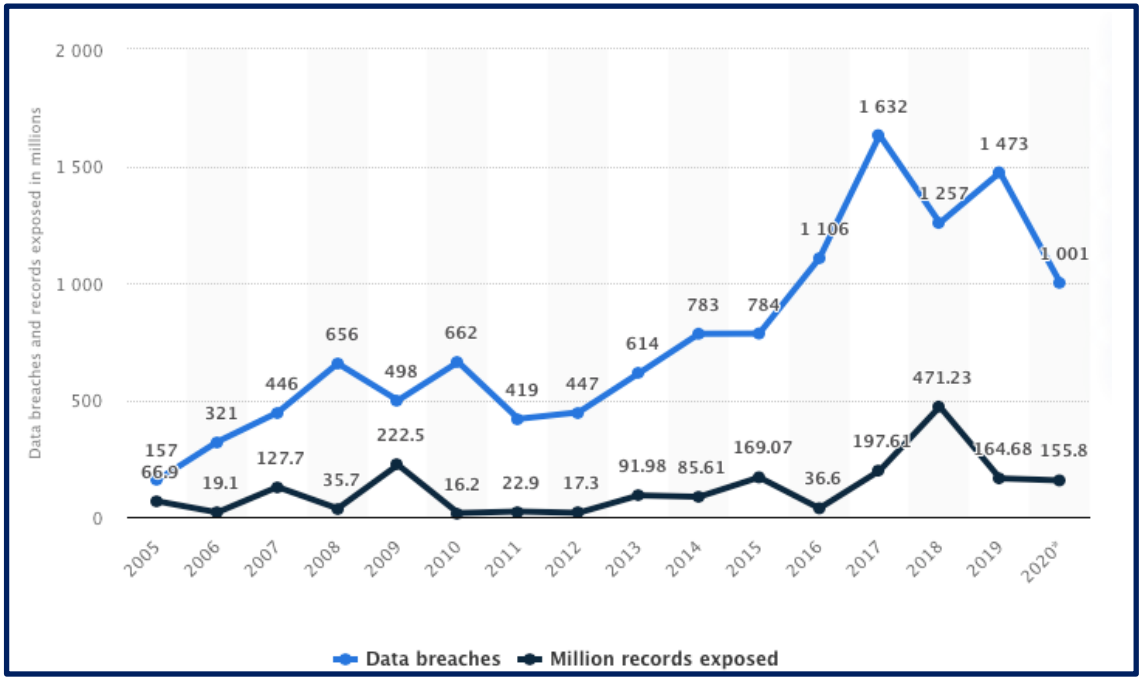
September 9, 2021

Jaeyoung Park

Postdoctoral researcher, Yonsei University

Asia Privacy Bridge Forum

Data Breaches



Company	Date of Breach Disclosure	Cost of Breach
Home Depot Inc	September 2014	$ 298,000,000
Target Corp	December 2013	292,000,000
TJX Companies Inc[1]	January 2007	220,900,000
Heartland Payment Systems	January 2009	147,600,000
Anthem, Inc.	February 2015	115,000,000
Global Payments Inc	March 2012	114,200,000
Equifax Inc[2]	September 2017	87,500,000
RSA Security (EMC Corp)	March 2011	66,300,000
Ubiquiti Networks, Inc.	August 2015	56,100,000
Mondelez International, Inc.[2]	June 2017	54,000,000

www.AuditAnalytics.com
1) Expanded population of breaches to 2007
2) New disclosure of cyber related costs/estimates

Source: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

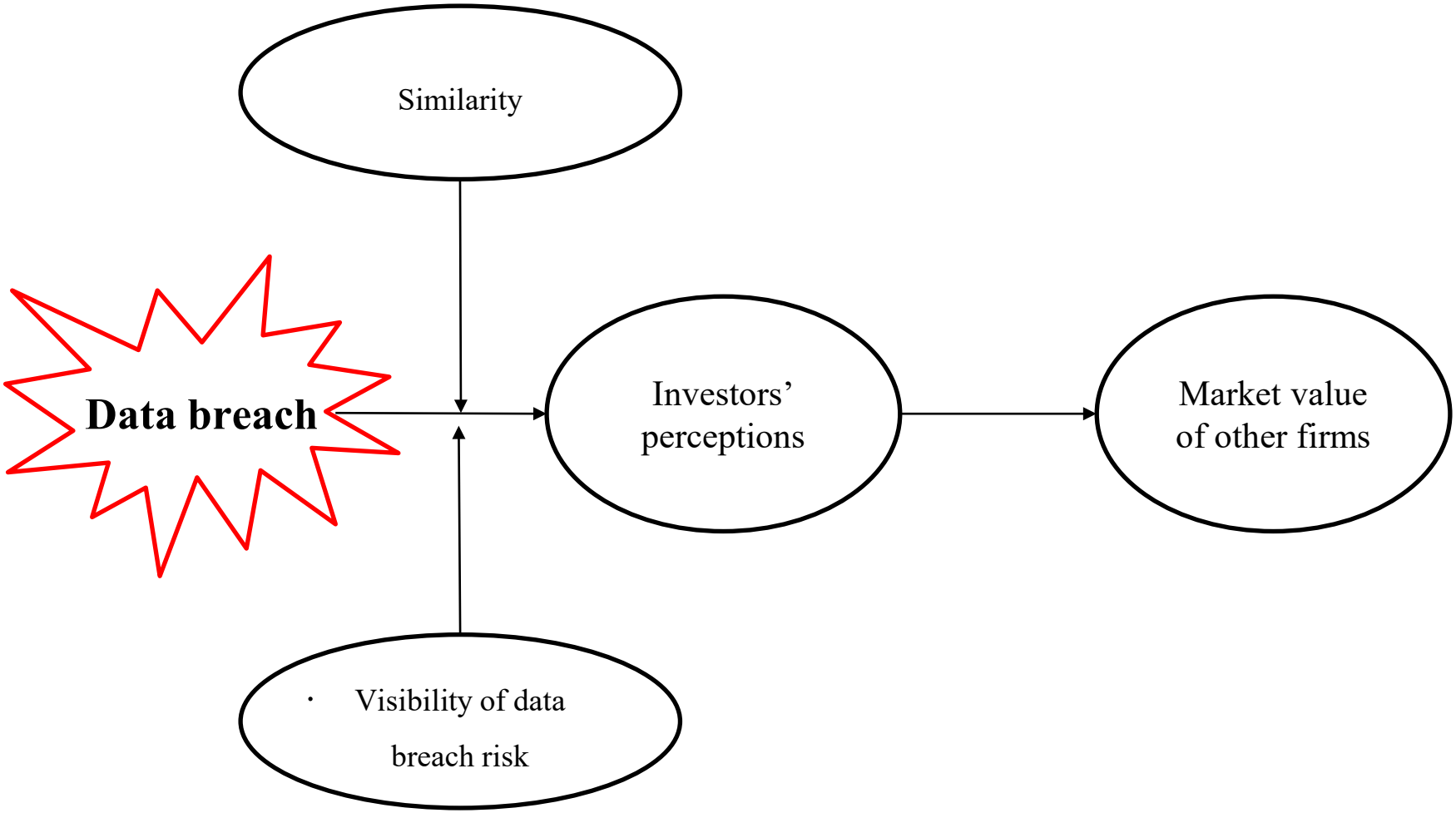
Source: https://blog.auditanalytics.com/ranking-the-equifax-data-breach-updated/

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

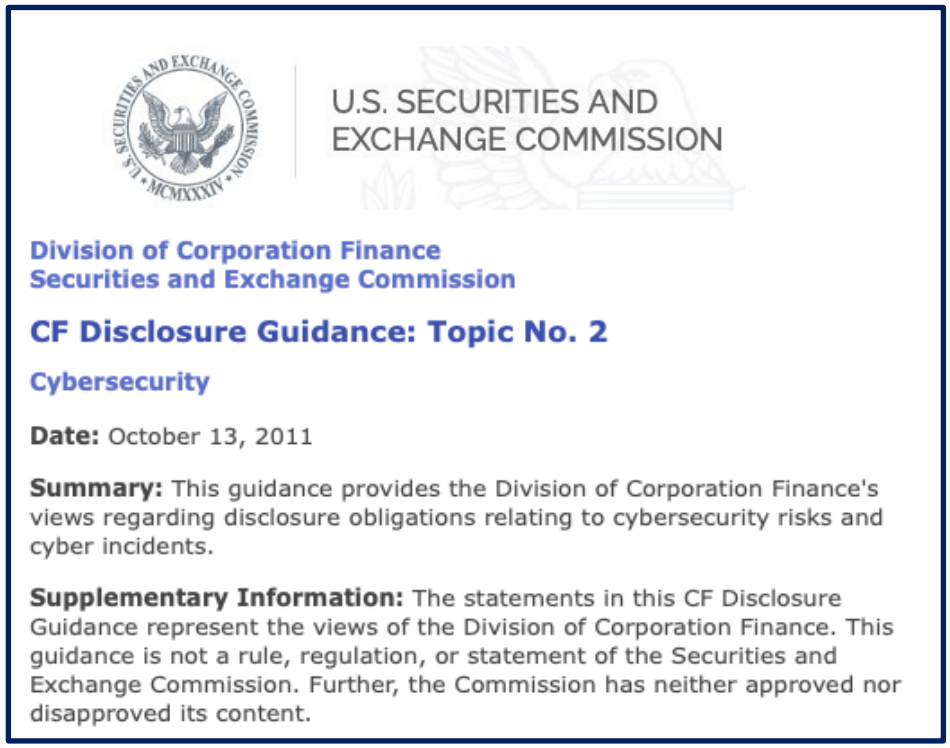


Theoretical Background: Information Transfer

- **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.**



U.S. SECURITIES AND EXCHANGE COMMISSION

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.

10-K Report

TABLE OF CONTENTS

An Example of Item 1A in 10-K Report (Target corporation)

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. -> "subcaption"

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."*

Method: Event Data (2013-2017)

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

Table 1. List of Breached Firms

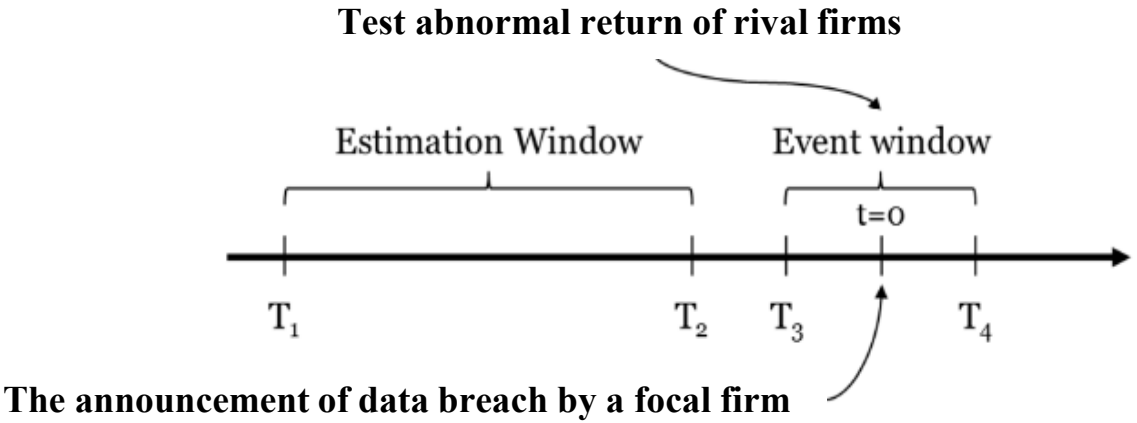
Event date	Event Firms	SIC	Asset [m$]	Employee	Revenue [m$]	Market value [m$]
20131219	Target	5331	48,163	361,000	73,301	38,982
20140305	Sally Beauty Holdings	5990	1,950	26,450	3,622	4,300
20140902	Home Depot	5211	40,518	365,000	78,812	106,053
20141021	Staples	5940	11,175	83,008	23,114	8,591
20150302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

Method: Sample (industry peers)

- Data source: COMPUSTAT 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.



Method: Definition of Variables

Table 2. Definition of Variables

Variable	Definition	Source
Dependent variable		
CAR (-1,1)	The cumulative abnormal return for the industry peers in the three days surrounding the data breach event	Eventus from WRDS
Independent variable		
Visible data breach risk	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.	EDGAR
Similarity	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.	Compustat from WRDS
Control variable		
Prior performance	The ratio of net income to total assets (Compustat annual item: NI/AT)	Compustat from WRDS
Firm size	Natural log of total assets in millions (Compustat annual item: AT)	Compustat from WRDS
Growth	The ratio between the book and the market value of firm's equity (Compustat annual item: CEQ/MKVALT)	Compustat from WRDS
Massive breach	Dummy variable, equal to 1 if non-breached firms is sample of the Target or Home Depot breach is, o otherwise.	PRC
Past breach	Dummy variable, equal to 1 if non-breached firms experience data breach(es) prior to the breach, o otherwise.	PRC

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

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

*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

Event window	Low similarity (N = 158)		High similarity (N = 152)		Difference test
	CAAR (%)	t-value	CAAR (%)	t-value	
(-1, 0)	0.126	.313	-1.480	-5.523***	3.295***
(0, 1)	0.160	.520	-1.077	-4.304***	3.108***
(-1, 1)	**0.173**	**.407**	**-1.602**	**-4.786*** **	**3.269*** **

*Note. CARs are calculated using the market model. The symbols *** denote statistical significance at the 0.1% levels.*

Results: The Role of Cybersecurity Risk Disclosure

- 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 5. Comparison Between Industry Peers by Data Breach Risk Disclosure

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

*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?