THE IMPACT OF DATA BREACH ON SUPPLIERS' PERFORMANCE: THE CASE OF TARGET

by

Tian Qi

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Consumer Science

West Lafayette, Indiana

May 2020

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Jiong Sun, Chair

Division of Consumer Science

Dr. Chun-Hung (Hugo) Tang

School of Hospitality and Tourism Management

Dr. Jonathan Bauchet

Division of Consumer Science

Approved by:

Dr. G. Jonathon Day

Dedicated to my family who raised me and supported me to chase my dream.

To my friends who listened to my troubles and comforted me.

To my boyfriend Yulong who supported me throughout the entire master program.

ACKNOWLEDGMENTS

I would like to acknowledge my committee chair, Dr. Jiong Sun, who generously and patiently spent countless time helping with data collection and analysis. This work would not have been possible without his continuous guidance.

Thank you Dr. Jonathan Bauchet and Dr. Chun-Hung (Hugo) Tang for agreeing to serve as a member of my committee.

Finally, I would like to appreciate all the professors who taught me and prepared me with enough knowledge to conduct this research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The author investigated the condition under which competition effect and contagion effect impact the suppliers of a firm encountering data breach. An event study was conducted to analyze the stock price of 104 suppliers of Target after the large-scale data breach in 2013. The result showed that suppliers with high dependence on Target experienced a negative abnormal return on the day after Target’s announcement, while those with low dependence experienced a positive abnormal return. After regressing the abnormal return on some explanatory variables, the result showed that firms with better operational performance and high information technology capability were less negatively affected. This study suggested that suppliers who relatively highly rely on one customer company are susceptible to the negative shock from that customer because of the contagion effect. Furthermore, maintaining good performance and investing in information technology can help firms reduce losses from negative events happened in customer companies.

INTRODUCTION

Entering the information age, industries rely more on a huge amount of data. Big data can enhance companies' decision making; however, it also brings forth security issues, making data security a major concern in this era. Due to various reasons including hacking, physical theft of the device, and human error, data breaches spring up. Based on the definition of the United States Department of Health and Human Services (2015), the data breach is "security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so". According to the report of Identity Theft Resource Center, there have been over 11,000 breaches since 2005, and the number of records exposed has reached 1.6 billion. Professor Ablon also did an internet-based survey in 2015 asking people their attitude towards data breaches from the consumer perspective. More than 6000 people participated. According to the result, 44% of people once received at least one breach notification in their lives, and 26% of them received it in the last 12 months. This implies that data breach happens frequently and is influencing a large number of people.

Data security has become an important concern not only for individuals but also for companies. According to a report of IBM Security in 2019, the average cost of data breaches in the U.S. is $8.19 million. Data breaches bring financial loss to corporations, as well as losing customers' confidence and causing reputational damage (Brown and Beltramini, 1989). Many studies have shown that data breaches have a negative impact on companies' stock performance. Journalist Bischoff found that the share price of companies who experienced data breaches "hit a low point approximately 14 market days following a breach" (2018). Another study (Acquisto, 2006) gives an analysis of 79 privacy information breaches incidents from 2000 to 2006, showing that data breaches have a short-lived negative impact on the corporation's market value. In addition, similar research did by Rosati and his colleagues (2017) using a sample of 87 data breaches events from 2011 to 2014 suggested social media has a significant effect on stock price after data breach announcement. In other words, the announcement on social media would worsen the negative effect on the stock price.

When the political firm Cambridge Analytica was reported to have access to private information of 50 million users on Facebook without consent in March 2018 (Granville, 2018), "Facebook stock plunged 8%" on March 19, which is the worst decline Facebook had experienced on a single day in the last six years (Chang, 2018). Furthermore, the stock of its rivals Twitter and Snap also got crushed. It shows that data breach could have a negative effect on both involved corporations and its competitors or other related companies. Although some research showed the impact of a data breach on the company encountering it, limited research has been conducted to study the impact on other relevant companies. Researchers Kashmiri and his colleagues (2017) studies the data breach of Target that happened in 2013. Their result showed that that event resulted in negative abnormal return for both Target and other U.S. retailers. They also investigated under what circumstances the contagion effect is more negative. Inspired by their research, The author aimed to use the same case to study the impact of a data breach on companies in another kind of relationship with the company encountering it, which is the relationship in the supply chain.

Companies in the supply chain network are integrated and interdependent. They share both profits and risks. If one company encounters a crisis, it may affect the rest of the entire supply chain and cause high costs. Supply chain relationship has various kinds of impact on a company's market reaction. The increasingly complicated supply chain network makes companies vulnerable to potential risks. Therefore, it is worth exploring whether data breaches will also affect companies in the supply chain network. To fill this gap, this paper used event study methodology to study the case of Target data breach in 2013 and investigate the influence of that event on Target's suppliers' stock performance.

On December 19, 2013, Target announced that 40 million payment card information of its customers have been accessed beyond authority, which was one of the most serious and largest credit and debit card breach. Because of the ignorance of warnings and unfamiliarity with malware detection service, Target's system was attacked by malicious software, and records were stolen (Shu, et al. 2017). The price of this incident is heavy. Target reported that in the fourth quarter of 2013, it spent $61 million in costs related to this data breach. In addition, after the massive data breach of Target was revealed, its stock had declined 11% (Cheng, 2014). The author wanted to investigate how did data breach influence firms in the supply chain network using the case of Target. For one thing, this data breach involves a large scale of records and has great social influence. For another, Target's suppliers are diverse, which contains firms in different sizes. Therefore, this case is appropriate for conducting this research.

For this study, the author addressed the following questions: Since Target data breach resulted in negative abnormal return for itself, what impact would it have on its suppliers? How did firm characteristics and supply-chain relationship characteristics reinforce or weakened this impact? Based on the literature review, the author argued that Target data breach caused negative abnormal return for its suppliers who had high dependence on Target as a result of contagion effect. Furthermore, suppliers with better operational performance (e.g. higher profitability and higher efficiency), greater IT capability and marketing capability (presence of CIO and CMO in top management teams), and weaker governance-related tie with Target are likely to have less negative impact.

After conducting the event study, this work showed correlation between suppliers' dependence on Target and abnormal return on the day after the announcement. Then an ordinary least squares regression model was built to test other hypotheses. Hypotheses that better operation performance (high gross profit to sales ratio, low SG&A to sales ratio and high return on equity), and high information technology capability could reduce the negative effect were supported by this study, while there was no evidence showing significant impact of marketing capability and suppliers' governance-related tie strength with Target.

LITERATURE REVIEW

Supply Chain Contagion

A phenomenon called supply chain contagion has been observed by prior research, which means that negative shock of an event can propagate through the company's supply chain network (Inoue and Todo, 2017; Inoue and Todo, 2019; Agca, et al., 2017). Negative events encountered by a company can cause significantly a negative impact on its suppliers' stock performance (Hertzel, et al., 2008; Hendricks, 2019). When encountering negative events, the sales and profit of a customer company decreased, which caused reduced demand for its suppliers. Previous research by Kashmiri and his colleagues established that Target data breach led to the loss of customer confidence, and their results showed Target experienced significantly negative abnormal return.

Boundary conditions

Factors that have influence on the level of supply chain contagion effect has been explored in the study of McFarland and his colleagues (2008). They found that the contact frequency was positively related to the level of contagion. The strength of supply chain relationship has also been observed to have impact on the intensity of contagion effect (Schiller, 2016). Relationship strength can be interpreted as supplier's dependence on customer companies, which can be measured through the percentage of revenue the supplier gets from a specific customer. As the percentage is larger, the supplier depends more on the customer, and therefore the crisis of customer would cause more significant impact.

Another important variable that may influence the effect of event is "Governance-related tie-strength" defined by Kashmiri (2017), which can be measured through institutional ownership overlap, "the proportion of the firm's shares held by institutions that also held shares of" the company encountering the data breach (p. 215). When an institutional investor hold shares of both supplier and customer companies, they would pay more attention to news that may have effect on other related companies, so that they would trade on such information (Cohen and Frazzini, 2008). In addition, as institutional investors maintain high level of ownership of the company and can participate in management decision making, they are considered as having more responsibility to help companies invest in value-adding initiatives (Carleton et al. 1998). If the company encountered data breach, the institutional investors would lose their reputation as monitor (Massa and Zaldokas 2012). In a result, other companies whose shares are held by those institutional investors are likely to face similar consequences.

Competition Effect

Different from contagion effect, competition effect occurs when an event happened to a company is considered as unique and not representative for other companies. In that case, the event is idiosyncratic, and investors would not expect similar events to happen in other similar firms. Under such circumstances, when a negative event take place in one company, the competitors of the company would receive more demands and therefore benefit from this event (Kashmiri, et al., 2017). It is common in grocery supply chains that suppliers serve both Target and its rivals at the same time. Therefore, when Target's rivals experienced a gain in their product demand, suppliers who were serving those rivals as well would get benefits.

Boundary conditions

When there is a crisis, investors' trust in a firm plays an important role. If investors have high level of trust on a firm, they will have more confidence about the company and are less likely to perceive investing in that firm as dangerous (Keh and Xie, 2008). A main source of Investor's trust and confidence is corporate performance. Investors are less likely to invest in a poorly operated company. Many measurements can be used to measure company's operational performance. Construct that indicates firm's profitability include gross profit ratio, return on assets, return on equity, and cost of goods sold to sales ratio. Furthermore, many variables like inventory turnover, return on investment, return on sales and SG&A to sales ratio represents company's efficiency. In addition, cash holdings can be interpreted as firm's level of freedom and ability to react to uncertainty. Firms with high profitability, efficiency and cash holdings are not only estimated to bring more benefits to investors in the future, but also are more likely to invest in information technology since they have enough money.

In term of data breach, suppliers' information technology capability could have large influence. Firms with advanced information technology and security system are perceived as having less possibility to leakage customers' data. According to the upper echelon theory (Hambrick and Mason, 1984), the structure of company's top management team is a great signal for company's system and behavior. If a CIO is present in the top management team, it suggests that the company is investing in IT system. Similarly, the presence of a CMO may indicate that the company has stronger crisis management ability when dealing with crisis, which can also be taken into consideration by investors.

In the case of Target, as it is a big customer, its crisis would have a significant impact on its suppliers, who are likely to experience financial interruption due to the financial loss Target would face. Nevertheless, competition effect may also exist in this case. Customers who felt disappointed about Target may turn to other retailers. Thus, Target's suppliers could gain more profit from the increasing demand from other retailers. It was previously observed that competition effect could offset contagion effect in some cases (Laux, 1998). Therefore, it is worth exploring the balance of competition effect and supply chain contagion in this case.

This paper aimed to examine the condition under which the supply chain contagion or competition effect overweighs each other and influences the effect of Target's data breach on its suppliers. Based on the above theories, the author proposed that suppliers' dependence on Target plays a major role in this case, which determines which effect is the main effect. When the percentage of revenues a supplier gains from a customer is large, the supplier is more susceptible for the loss of demand from that customer due to the negative shock, in which case contagion effect play a major role. When the percentage of revenues a supplier gains from a customer firm is small, the supplier has low dependence on that customer and gains more revenue from competing customers. The competition effect benefits competing firms whose sales increase. The effect in turn benefits the upstream suppliers and overweighs the contagion effect. Moreover, other firm characteristics like operational performance, IT and marketing capability, and governance related tie strength could affect the intensity of the net effect. To be specific, the following hypotheses were made:

Hypothesis 1: After Target announced the data breach, suppliers with lower percentage of revenue coming from Target will have positive abnormal return due to competition effect, while those with higher percentage will have negative abnormal return as a result of contagion.

Hypothesis 2: When suppliers have better operational performance, the negative effect of Target's data breach is less pronounced.

Hypothesis 3: The presence of CIO and CMO in suppliers' top management team makes the negative effect of Target's data breach less pronounced.

Hypothesis 4: When suppliers' governance-related tie strength with Target is weak, the negative effect of Target's data breach is less pronounced.

METHODS

Sample

The list of Target's suppliers along with their ticker and percentage of revenue coming from Target in the year of 2013 was obtained through the Bloomberg database. There are initially 356 quantified and unquantified suppliers in total. As this paper aims to study the impact on suppliers, Target Corporation was not included. Then, after removing non-listed companies and companies with missing percentage of revenue, the final dataset for event study contains 104 samples. Since this study aims to investigate how suppliers' dependence on Target influences their abnormal return, suppliers are divided into 3 groups. To be specific, they are sorted according to their percentage of revenue coming from Target and then divided equally; however, as some firms on the boundary have the same percentage and firms with the same percentage should be in the same group, the number of firms in each group was not exactly equal.

Then, after matching those remaining firms with their firm characteristics data from Compustat database, 23 companies were removed because of missing information. So, the dataset for regression contains 81 samples. Table 1 provides the summary statistics of this dataset.

Table 1 Summary Statistics

	Obs.	Mean	St. Deviation	5%	25%	Median	75%	95%
SIZE	81	8.00	2.03	4.43	6.74	8.32	9.50	11.36
COGS	81	0.60	0.16	0.31	0.53	0.62	0.72	0.86
GP/SALE	81	0.39	0.16	0.14	0.28	0.38	0.47	0.69
SG&A	81	0.23	0.11	0.06	0.15	0.23	0.31	0.42
ROA	81	0.06	0.11	-0.12	0.04	0.07	0.11	0.15
ROE	81	-0.00	0.32	-0.38	0.04	0.05	0.07	0.14
ROI	81	0.07	0.23	-0.28	0.06	0.11	0.17	0.26
ROS	81	0.06	0.09	-0.11	0.04	0.08	0.10	0.19
CIO	81	0.29	0.45	0	0	0	1	1
CMO	81	0.41	0.49	0	0	0	1	1
CASH	81	0.14	0.15	0.01	0.03	0.08	0.20	0.39
INVT	81	7.61	8.27	2.39	3.75	5.26	7.13	23.46
INVESTOR	81	0.75	0.16	0.43	0.71	0.80	0.85	0.92
REVENUE	81	0.03	0.07	0.00	0.00	0.01	0.03	0.12

Event Study

This paper used event study methodology to investigate the impact of Target data breach event on suppliers' stock performance. The stock price of each public company was downloaded from Yahoo Finance. Then, market model was used to calculate abnormal returns of each company:

$$E(R_{it}) = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$$

where $E(R_{it})$ is the expected return of company i on day t if the event does not occur; α_i and β_i was estimated using regression model over 200 trading days before the event date and reflected the correlation between the stock price of company i with that of the market. The daily abnormal return of each supplier is calculated as:

$$AR_{it} = R_{it} - E(R_{it})$$

where R_{it} is the actual return of company i on day t, which is the difference between actual return and expected return. Since multiple companies are involved in this study, the average abnormal return of each group was calculated to indicate the average reactions of suppliers on a specific day. The equation is:

$$AAR_t = \frac{1}{N}\sum_{i=1}^{N} AR_{it}$$

In addition. cumulative average abnormal return of each group is calculated to reflect the average abnormal return during a period. It was computed as:

$$CAR_i[t_1, t_2] = \sum\nolimits_{t_1}^{t_2} AAR_{it}$$

which is the sum of company i's average abnormal return over the window $[t_1, t_2]$. Finally, the cumulative average abnormal return of suppliers was tested using t test and compared between groups.

Ordinary Least Squares Regression Model

Dependent Variable

Target officially announced the data breach event on December 19, 2013, which is regarded as the event day (t = 0); It is shown in the Figure 1 that according to Google Trends the searches of keywords related to Target data breaches increased dramatically on December 19. The cumulative average abnormal return of multiple event windows was calculated in order to find the most significant one. Then the abnormal return of each supplier was regressed on proposed explanatory variables. In this step, all three groups are considered together in one model, because the size of each single group was too small to give representative result; however, the author still provided the results of each group in Appendix for reference.

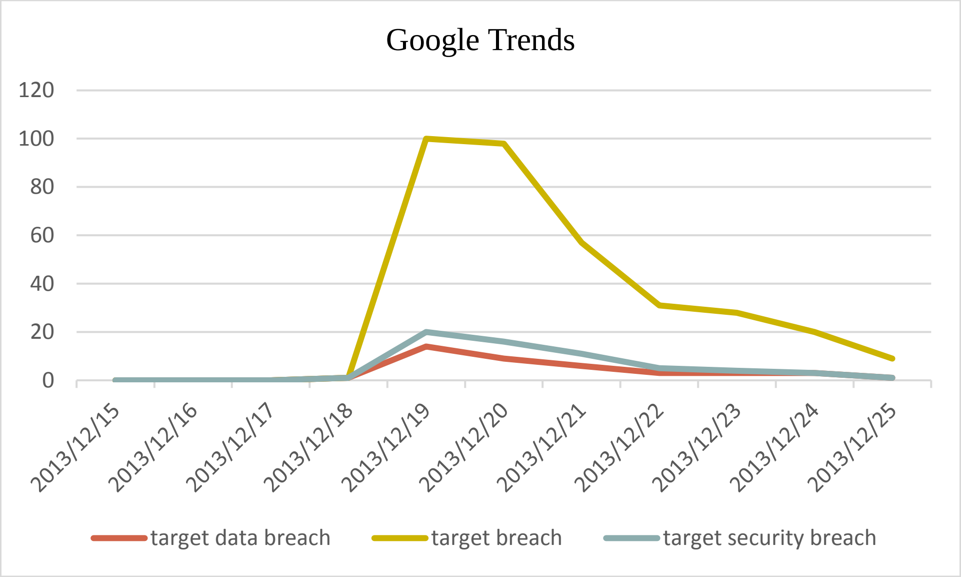

Figure 1 Google Trends of “Target data breach”, “Target breach” and “Target security breach”

Independent Variables

The independent variables of suppliers in the year prior to the data breach (fiscal year 2012) were collected. The measurement of each variable and the data source are provided in table 2.

Table 2 Measurement of Variables

Variable Name	Measures	Source
Firm Size (SIZE)	Natural logarithm of the firm’s total assets log (AT)	CRSP
COGS / Sale	Cost of goods sold divided by total sales	CRSP
Gross profit to total sales (GP / Sale)	(Total revenue - cost of goods sold) / Total sale (REVT – COGS) / SALE	CRSP

SG&A / Sale	Total selling, general, and administrative expenses / total sales XSGA / SALE	CRSP
Return on Assets (ROA)	Net income / total assets	CRSP
Return on Equity (ROE)	Net income / equity	CRSP
Return on Investment (ROI)	Net income / total invested capital	CRSP
Return on Sales (ROS)	Net income / revenues	CRSP
CIO	Presence of a CIO in a firm's top management teams. Dummy variable	10-K Filings
CMO	Presence of a CMO in a firm's top management teams. Dummy variable	10-K Filings
Cash Holding (CASH)	Assets hold in cash CHE / AT	CRSP
Inventory Turnover (INVT)	Cost of goods sold / average inventory $\mathrm{COGS}/(INVT_t - INVT_{t-1})/2$	CRSP
Institutional Ownership Overlap (INVESTOR)	Shares held by institutions that also held shares of Target / total shares	Thomson Reuters
%Revenue (REVENUE)	Percentage of revenues coming from a specific customer	Bloomberg

Control Variables

The author controlled each supplier's firm size and percentage of revenue coming from Target as they were influential but were not studied in this case. Table 3 shows the correlation between those explanatory variables and descriptive statistics. The following regression model was employed:

$$\begin{aligned} AR_i = \beta_0 &+ \beta_1\, SIZE_i + \beta_2\, COGS/SALE_i + \beta_3\, GP/SALE_i + \beta_4\, SG\&A/SALE_i + \beta_5\, ROA_i \\ &+ \beta_6\, ROE_i + \beta_7\, ROI_i + \beta_8\, ROS_i + \beta_9\, CIO_i + \beta_{10}\, CMO_i + \beta_{11}\, CASH_i \\ &+ \beta_{12}\, INVT_i + \beta_{13}\, INVESTOR_i + \beta_{14}\, REVENUE_i \end{aligned}$$

Table 3 Variable Correlation and Descriptive Statistics

Variable	1	2	3	4	5	6	7	8	9	10	11	12	13	14
SIZE	1													
COGS	-.3	1												
GP/SALE	.3	1	1											
SG&A	.0	-.8	.8	1										
ROA	.3	-.2	.2	-.0	1									
ROE	.2	-.0	.0	-.0	.8	1								
ROI	.3	-.2	.2	-.0	.9	.8	1							
ROS	.4	-.4	.4	.0	.8	.7	.7	1						
CIO	.2	-.0	.0	-.0	.1	.0	.1	.1	1					
CMO	.2	-.1	.1	.1	.1	.0	.1	.1	.5	1				
CASH	-.1	-.1	.1	.0	.2	.1	.1	.2	.0	-.0	1			
INVT	-.0	.0	-.0	-.1	.0	.0	-.0	.0	-.0	-.0	.4	1		
INVESTOR	-.0	.0	-.0	-.0	-.0	-.0	-.0	-.0	-.3	-.1	.0	.0	1	
REVENUE	-.3	.0	-.0	.0	-.1	-.1	-.1	-.2	-.0	-.0	.3	.1	.0	1
Mean	8.07	.61	.39	.24	.06	-.01	.07	.06	.28	.41	.14	7.6	.76	.03
St. Deviation	2.03	.16	.16	.11	.11	.32	.23	.09	.45	.50	.15	8.26	.16	.07

RESULTS

The result from event study was that only the average abnormal return (AAR) on Day 1 (December 20) is significant for all groups based on t test, which suggested correlation between suppliers' dependence on Target and abnormal return. As the figure shows, the abnormal return for suppliers with lower percentage of revenue coming from Target was 0.76% with a significance level of 5%; the abnormal return for supplies with medium percentage of revenue coming from Target was not significant; and the abnormal return for suppliers with high percentage of revenue coming from Target was -0.34% with a significance level of 10%. Therefore, suppliers with lower dependence on Target experienced positive abnormal return, while those with higher dependence had negative abnormal return. It supported the hypothesis that suppliers with lower percentage of revenue coming from Target will have positive abnormal return due to competition effect, while those with higher percentage will have negative abnormal return as a result of contagion.

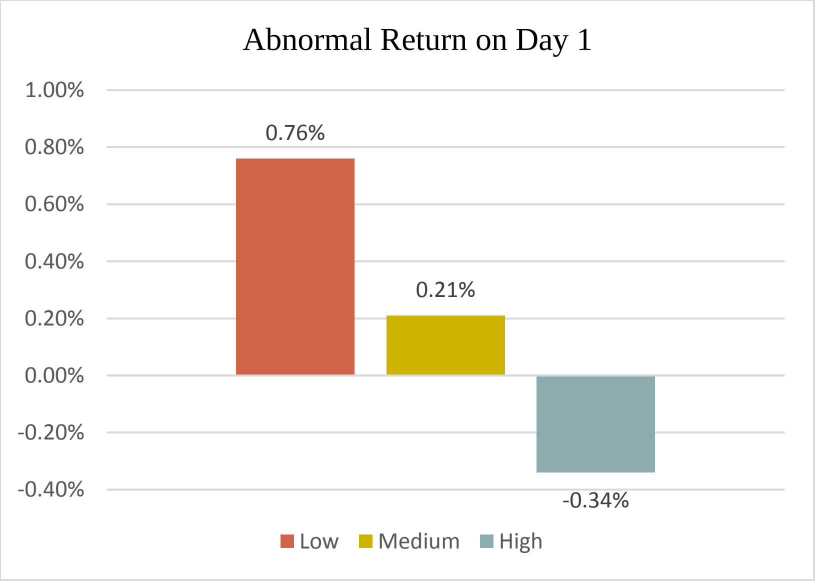

Figure 2 Result from Event Study

Then, the result of regressing the average abnormal return on Day 1 on chosen explanatory variables was provided in Table 4. The overall model is significant with a significance level of 5%. The overall R-square of this model is 28.6%, which means this model explains a fair number of variances compared with other similar research. Besides control variable, the gross profit to sales ratio, selling, general, and administrative expenses to sales ratio, return on equity and the presence of CIO in top management team has significant influence. The sign of variable coefficient indicates whether they are positively or negatively correlated with abnormal return. Since high gross profit to sale rate, high return on equity and low selling, general, and administrative expenses to sales ratio means better profitability and efficiency, the hypothesis was supported that when suppliers have better operational performance, the negative effect of Target data breach is less pronounced. Furthermore, the presence of CIO is positively correlated with abnormal return, therefore the hypothesis was supported that high IT capability makes the negative effect of Target data breach less pronounced. Since other variables are not significant, there was no evidence supporting the hypothesis about marketing capability and governance related tie strength with Target.

Table 4 OLS Regression Result

Variables	Coefficient
COGS/Sale	-0.02
GP/Sale	0.06**
SG&A/Sale	-0.1**
ROA	-0.01
ROE	0.04**
ROI	-0.02
ROS	-0.1
CIO	0.01**
CMO	0.00
Cash holding	0.02
INVT	-0.00
INVESTOR	0.00
SIZE	-0.00**
REVENUE	-0.03

** $p < 0.05$, * $p < 0.1$

DISCUSSION AND CONCLUSION

In conclusion, this study shows that in the case of Target data breach, suppliers' dependence on Target determines which effect they experienced. Suppliers with lower percentage of revenues coming from Target experienced positive abnormal return due to competition effect between Target and other retailers. Suppliers with high percentage experienced negative abnormal return due to contagion effect. This study also shows that suppliers with better operational performance and higher IT capability experienced less negative effect from Target data breach. It can give companies insights that instead of relying on one big customer, they could serve more customers and decrease their dependence on each customer, so that they would not experience great losses due to negative shock from customers. Furthermore, maintaining good performance and investing more in information technology and security system can reduce the negative effect of a data breach happened to a connected company.

This study contributed that it provided insights about how a company's data breach influences its supply chain partners especially suppliers. As for future research, since this study only investigated the case of Target, the result may not be generalized to other supply chain relationships. Thus, more events should be studied in order to generalize the findings of this study.

APPENDIX A. RESULTS OF REGRESSION IN GROUPS

Table 5 Regression Results for Group with Low Dependence

Variables	Coefficient
COGS/Sale	-0.05
GP/Sale	0.07
SG&A/Sale	-0.08
ROA	0.12
ROE	0.15
ROI	-0.08
ROS	-0.31
CIO	0.00
CMO	0.02
Cash holding	0.05
INVT	0.00
INVESTOR	0.11
SIZE	-0.00
REVENUE	1.42

Table 6 Regression Results for Group with Medium Dependence

Variables	Coefficient
COGS/Sale	0.04
GP/Sale	-0.09
SG&A/Sale	0.08
ROA	-0.78
ROE	-0.44
ROI	0.55*
ROS	0.19

CIO	0.02*
CMO	-0.01
Cash holding	0.02
INVT	-0.00*
INVESTOR	0.06
SIZE	-0.00
REVENUE	0.33

Table 7 Regression Results for Group with High Dependence

Variables	Coefficient
COGS/Sale	0.03
GP/Sale	-0.07
SG&A/Sale	0.19
ROA	0.22
ROE	-0.01
ROI	-0.07
ROS	0.17
CIO	-0.00
CMO	0.00
Cash holding	-0.06*
INVT	-0.00
INVESTOR	-0.02
SIZE	-0.00
REVENUE	0.11

REFERENCES

Ablon, L., Heaton, P., Lavery, D., & Romanosky, S. (2016). *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information.* RAND Corporation.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

Agca, S., Babich, V., Birge, J. R., & Wu, J. (2017, December 4). Credit risk propagation along supply chains: Evidence from the CDS market. *Georgetown McDonough School of Business Research Paper*, (3078752).

Bischoff, P. (2018, September 6). Analysis: How data breaches affect stock market share prices. Comparitech. Retrieved from https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/

Bloomberg. *Bloomberg Professional*. [Online]. Available at: Subscription Service

Brown, S. P., & Beltramini, R. F. (1989). Consumer complaining and word of mouth activities: field evidence. *Advances in Consumer Research, 16*(1), 9–16.

Carleton,W. T., Nelson, J. M., & Weisbach, M. S. (1998). The influence of institutions on corporate governance through private negotiations: evidence from TIAA-CREF. *Journal of Finance, 53*(4), 1335–1362.

Chang, S. (2018, March 30). Facebook Data Breach: Twitter and Snap Stock Tumble on News. *Investopedia*. Retrieved from https://www.investopedia.com/news/facebook-data-breach-twitter-and-snap-stock-tumble-news/

Cheng, A. (2014, February 26). Two months after damaging data breach, Target stock has its best day in 5 years. *MarketWatch*. Retrieved from http://blogs.marketwatch.com/behindthestorefront/2014/02/26/two-months-after-damaging-data-breach-target-stock-has-its-best-day-in-5-years/

Cohen, L., & Frazzini, A. (2008). Economic links and predictable returns. *Journal of Finance, 63*(4), 1977–2011.

CRSP/Compustat Merged. *CRSP/Compustat Merged. Center for Research in Security Prices*. [Online]. Available at: WRDS http://wrds-web.wharton.upenn.edu/wrds/

Granville, K. (2018, March 19). Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. *The New York Times.* Retrieved from https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Hambrick, D. C., & Mason, P. A. (1984). Upper echelons: the organization as a reflection of its top managers. *Academy of Management Review, 9*(2), 193–206.

Hendricks, K. B., Jacobs, B. W., & Singhal, V. R. (2019). Stock market reaction to supply chain disruptions from the 2011 Great East Japan Earthquake. *Manufacturing & Service Operations Management.*

Hertzel, M. G., Li, Z., Officer, M. S., & Rodgers, K. J. (2008). Inter-firm linkages and the wealth effects of financial distress along the supply chain. *Journal of Financial Economics, 87*(2), 374-387.

IBM Security. (n.d,). *Cost of a Data Breach Report*. Retrieved from https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.123576911.596650498.1588245294-942065689.1588245294

Identity Theft Resource Center. (n.d.). *Data Breaches*. Retrieved March 18, 2020, from https://www.idtheftcenter.org/data-breaches/

Inoue, H., & Todo, Y. (2017). Propagation of negative shocks through firm networks: Evidence from simulation on comprehensive supply-chain data. Available at SSRN 2932559.

Inoue, H., & Todo, Y. (2019). Firm-level propagation of shocks through supply-chain networks. *Nature Sustainability, 2*(9), 841-847.

Kashmiri, S., Nicol, C. D., & Hsu, L. (2017). Birds of a feather: intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science, 45*(2), 208-228.

Keh, H. T., & Xie, Y. (2009). Corporate reputation and customer behavioral intentions: The roles of trust, identification and commitment. *Industrial Marketing Management, 38*(7), 732-742.

Laux, P., Starks, L. T., & Yoon, P. S. (1998). The relative importance of competition and contagion in intra-industry information transfers: An investigation of dividend announcements. *Financial Management*, 5-16.

Massa, M., & Zaldokas, A. (2012). Information transfers among co-owned firms. *American Finance Association Meeting*.

McFarland, R. G., Bloodgood, J. M., & Payan, J. M. (2008). Supply chain contagion. *Journal of Marketing, 72*(2), 63-79.

Rosati, Cummins, Deeney, Gogolin, Van Der Werff, & Lynn. (2017). The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. *International Review of Financial Analysis*, *49*(C), 146-154.

Schiller, C. M. (2016). The Global Propagation of Economic Shocks: Financial Contagion along International Supply-Chains.

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017, January 18). Breaking the target: An analysis of target data breach and lessons learned. *arXiv preprint arXiv:1701.04940.*

Thomson Reuters Institutional (13f) Holdings. *Thomson Reuters*. [Online]. Available at: http://wrds-web.wharton.upenn.edu/wrds/

United States Department of Health and Human Services. (2015, July 1). Retrieved from https://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf