Both Sides of the Coin:
The Impact of Cyber Attacks on Business Value

Keman Huang, Rebecca Ye, Stuart Madnick

Working Paper CISL# 2019-25

December 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Both Sides of the Coin: The Impact of Cyber Attacks on Business Value

Keman Huang, Rebecca Ye, Stuart Madnick
Cybersecurity at MIT Sloan, MIT
Sloan School of Management, MIT
keman@mit.edu, rebecca.ye@wellesley.edu, smadnick@mit.edu

Abstract: Cyber incidents are hitting companies and making news headlines almost every day. It is critical to investigate the impacts of these incidents on the organizations' business value. The stock price, a widely used measurement of business value, of every victimized company fluctuates differently after a data breach. This article summarizes the factors that drive the whirling of the coin and suggests more proactive cyber crisis management to turn incidents into opportunities to create positive long-term impacts and enhance cyber resilience.

Stock Prices Fluctuate Differently After Data Breaches

In the wake of the recent Capital One hack, the company's stock price noticeably dropped. Though the short-term stock loss initially seemed significant, the damage appears less dramatic from a six-month window. This raises questions: can Capital One make a complete stock recovery in the long-term? If so, can cyber incidents just be seen as a nuisance with limited impact on the business?

Following the announcement of the Equifax breach back in early September of 2017, the company saw a similar negative reaction from the stock market. Equifax's stock prices plunged from 141.59 USD to 92.89 USD in just two weeks. As of August 2019, nearly two years after the attack, Equifax has recovered to its pre-breach stock value. However, in comparison with the index fund for the NASDAQ Financial-100, Equifax's stock value was roughly in line with the index fund prior to the breach, but dropped well below the fund following the breach. Though the gap between Equifax's stock value and the index fund's stock value has gradually closed in, Equifax's stocks still remain significantly lower than the index fund value of the NASDAQ Financial-100. Whether Equifax will make a full stock value recovery in the long-term is still up for debate.

However, Target and TJ Maxx are seeing record profits today, despite their highly publicized past breaches. The JP Morgan Chase breach didn't impact the long-term stock growth at all. The stock price for Banco Inter, on the contrary, actually rose right after a data breach incident. These conflicting observations indicate a need for an in-depth understanding of cyber incidents' impact on business value: what factors are driving the different outcomes from data breach incidents?

Investigating the damage inflicted by cyber security breaches to firms is critical for minimizing financial losses and understanding how we can more effectively engage companies to develop their strategies to mitigate those impacts. If cyberattacks are damaging to business value in the long-term, then businesses will be more motivated to invest more in digital security. But if cyberattacks in fact have no long-term damage to business value, companies may be de-incentivized from developing cybersecurity.

Stock price has been widely use to evaluate business value. Prior efforts have been conducted to study the impact of data breach incidents on stock prices. To have a better understanding about the state-of-the-art, using combinations of key words and phrases, such as: “cyber”, “breach”, “firm”, “market value”, and “stock”, we are able to locate prior studies as summarized in the Appendix. Not surprisingly, we again see inconsistent conclusions; the negative impact on the stock price from data breach incidents can be limited, especially in the long-term, while some of the time no significant impacts can be observed.

Negative Short-term Impact from Data Breach Incidents

A large portion of these studies reveal some stock reductions, especially in the short-term, from the data breach incidents. Garg etc. [1] are able to quantify the short-term impact that firms affected by a cyber breach experienced as a 2.7% decline in their stock price relative to the overall market on the day following the attack. Based on the studies on 24 companies publicly listed on the NYSE, Bischoff [2] shows that in the long-term, companies that were breached underperformed the market. Finance and payment sectors saw the greatest reductions, while the healthcare sector was least affected. Arcuri etc. [3] find that there is a significant overall negative market reaction to announcements of security breaches and the negative impact is more significant amongst firms in the financial sector. There is even a negative market reaction to firms prior to the announcement of the attack, suggesting the existence of insider trading.

The characteristics of individual data breach incidents, including the value of the underlying assets and the firm size, can also affect the negative impact. Using identified information security breaches between 1995-2000, Campbell etc.[4] identify the negative market reactions to information security breaches involving confidential data, but the reactions are insignificant when confidential information is not involved. Ko, Osei-Bryson & Dorantes [5] further explore impacts of each type of breach and IT intensity, showing that breaches affecting information confidentiality and availability have long-term negative impacts while breaches involving information integrity may experience immediate negative stock reactions, but the damage does not persist in the long-run. Kamiya etc. [6] reveals that firms that suffer attacks on customers’ personal financial information experience equity value losses $1.06 billion greater than breaches not involving personal financial information. Cavusoglu etc. [7] confirms that firm announcements of internet security breaches are negatively associated with stock market levels. Though security breaches negatively impact all victimized firms, breaches are particularly damaging to smaller firms’ survivability.

None or Evanescent Long-term Impacts from Data Breach Incidents

Some studies argued that the impact of data breach incidents on data breach incidents can be very limited. Hovav & D'Arcy’s early study [8] in 2004 shows that markets do not penalize firms affected by cybersecurity breaches, resulting in a lack of incentive for managers to develop their cyber security. Kvochko & Pant [9] argue that data breaches don't hurt stock prices, as the medium and long-term impact on companies’ profitability is arguable and need more empirical evidence.

The study [10] on firms listed on S&P 500 conducted in 2018 shows that in the financial sector, there is strong

evidence of firm reaction in the short-term, but the effects dissipate long-term. For industrial, information technology, and health sectors, firm reactions to cyber attacks are actually insignificant.

Collecting data on cyber attack costs through surveys and interviews with industry representatives across sub-sectors: banking, cards, insurance, retail, online payment providers, financial services, and government fraud service, as well as using system dynamics methodology to build a causal loop diagram, Lagazio etc. [11] concludes that effective strategies to protect a company's business interests and market positioning in the event of cyber incident can also minimize the costs of the attack.

The study from Gordon etc. [12] shows that the attitude toward breaches seems to have shifted towards that of a nuisance as opposed to an economic threat. Since organizations and the market are getting used to the recurrence of data breach incidents, and consumers continue to buy, the impact can be limited and this attitude may even result in neglected risk management issues in firms' critical digital infrastructures.

Factors Beneath the surface that Drive the Whirling of the Coin

These existing studies again confirm our first impression about the conflict observations: some firms continue to experience reverberations from the attack, even years after; some can make full recoveries in the long term while the short term impact may be limited. As summarized in Table 1, the market consequences of attacks may differ depending on the industry, firm size, and the type of information breached: confidentiality, integrity, or availability, the response strategy and the attitude shift from considering cyberattacks an economic threat, to viewing cyberattacks as a nuisance. A company's response and recovery behaviors to the data breaches can turn those incidents into opportunities to improve and optimize their business like increasing transparency, enhancing cybersecurity maturity to implement competitive advantages, optimizing the digital strategy etc. After the JP Morgan Chase breach, the company released extensive information on the attack and doubled its investment in security. Companies are recognizing the cyber risk within their annual reports, considering cybersecurity as part of their corporate social responsibility to build social trust, and hiring more cybersecurity professional to enhance internal cybersecurity capabilities, especially after they are affected by data breach incidents.

Table 1: Factors Affect the Long-term Impact of Data Breach Incidents

Contributes to Negative Long-Term Impacts	Reduces Negative Long-Term Impact
Sector: Financial	**Sector:** Industrial, Information Tech & Health
Information: Confidentiality & Availability	**Information:** Integrity
Organization: Firm Size	**Organization**: Investments and recovery strategies; **Customer**: Attitude Shift

Beyond these factors, the cultural attitudes toward cyber breaches can make the stock reactions to data breach incidents vary globally. Cultural perceptions may cause investors to blame the company for poor security management as opposed to seeing the company as a victim of an inevitable attack.

Furthermore, stock prices may be a widely accessible measure of business value, but they are often influenced by

emotional or even irrational reasoning, and therefore may not be the most effective way to analyze business value impact. Investors may negatively respond to cyberattacks under the sole assumption that cyberattacks always damage company revenue and earnings. But what if the assumption is false? It is possible that sales do not drop at all after an attack, or even increase as a result of the attack, just like the Target, TJ Maxx and Banco Inter example. A possible explanation for the increased profits could be that the attacked companies were aggressively implementing new technologies, which made them vulnerable to attacks. But in the long run, any damages from the attack dissipated under the economic benefits of their technological innovations.

Never Waste a Good Crisis: Turning a Bad Thing into a Good Thing

It is often said that there are only two types of companies: those that have been hacked and those that will be [13]. This inevitable characteristic of cyber incidents emphasizes the necessity to effectively respond to incidents and manage the short-term and long-term impact. Many previous studies already confirm the short-term stock price reduction due to the cyber incident but this can be impacted by different factors such as industry, type of cyber breach and response strategy. More data to better assess these factors will be valuable to effectively manage the short-term negative impact.

More importantly, the long-term impact of cyber incidents on stock price is still inconclusive; the mostly negative, if not significant, impact indicates that those organizations do not effectively turn cyber incidents into opportunities to improve and optimize their business. Just as quoted from Winston Churchill: “Never Waste a Good Crisis”. While the cyber incident brings the victimized company to the spotlight, it provides free public exposure for the company to showcase their responsibility and efforts to protect their stakeholders, customers, suppliers, and community. Reducing the cyber incident’s potentially negative impact and turning it into a positive impact on the organization’s long-term digital innovation, should be a mission for every organization.

Stock price is used in most studies as a indicator for business performance. But, it is possible that investors, worried about a drop in business, cause the stock price to drop, but actual consumers continue to buy. It would be interesting to measure actual business impact (such as sales volume), both short-term and long-term. The whole community, the business leaders, researchers, and stakeholders, should accept such a challenge and both envision and resolve to learn from cyber incidents to enhance the society’s cyber resilience.

Reference

[1] Garg, A., Curtis, J. and Halper, H. (2003). “Quantifying the Financial Impact of IT Security Breaches: What Do Investors Think?”. Information Management & Computer Security 11(2): pp. 74-83.

[2] Bischoff, P. (2018). “Analysis: How Data Breaches Affect Stock Market Share Prices (2018 update)”. Comparitech. https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/

[3] Arcuri, M., Brogi, M. and Gandolfi, G. (2017). “How does cyber crime affect firms? The effect of information security breaches on stock returns”. CEUR-WS 1816. http://ceur-ws.org/Vol-1816/paper-18.pdf

[4] Campbell, K., Gordon, L., Loeb, M. P. and Zhou, L. (2003). “The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market”. Journal of Computer Security 11(3): pp. 431-448.

[5] Ko, M., Osei-Bryson, K. and Dorantes, A. (2009). Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms. Information Resources Management Journal 22(2): pp. 1-21.

[6] Kamiya, S., Kang J., Kim, J., Milidonis, A. and Stulz, R. M. (2018). What is the Impact of Successful Cyberattacks on Target Firms?. NBER Working Paper 24409. https://www.nber.org/papers/w24409.pdf

[7] Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004). "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers". International Journal of Electronic Commerce 9(1): pp. 70-104.

[8] Hovav, A. and D'Arcy, J. (2004). "The Impact of Virus Attack Announcements on the Market Value of Firms". Information Systems Security 13(3): pp. 32-40.

[9] Kvochko, E. and Pant, R. (2015). "Why Data Breaches Don't Hurt Stock Prices". Harvard Business Review. https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

[10] Tweneboah-Koduah, S., Atsu, F. and Buchanan, W. J. (2018). "Impact of Cyberattacks on Stock Performance: A Comparative Study". Information and Computer Security 26(3).

[11] Lagazio, M., Sherif, N. and Cushman, M. (2014). "A multi-level approach to understanding the impact of cyber crime on the financial sector". Computers & Security 45, pp. 1-32.

[12] Gordon, L. A., Loeb, M. P. and Zhou, L. (2011). "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?". Journal of Computer Security 19(1): pp. 33-56.

[13] Richard Bejtlich (2018), The Origin of the Quote "There Are Two Types of Companies", https://taosecurity.blogspot.com/2018/12/the-origin-of-quote-there-are-two-types.html

Appendix

A. Studies that found long-term stock reduction

Title	Summary	Data	Author(s)	Source
The economic cost of publicly announced information security breaches: empirical evidence from the stock market (2003)	Markets have a negative reaction to information security breaches involving confidential data, but the reaction is not significant when confidential information is not involved. The market impact of security breaches depends heavily on the value of the underlying assets.	Searched Wall Street Journal, New York Times, Washington Post, Financial Times and USA Today for breaches 1995-2000. Used Center for Research in Security Prices (CRSP) database for returns history.	Campbell, Gordon, Loeb & Zhou	https://www.researchgate.net/publication/220065342_The_Economic_Cost_of_Publicly_Announced_Information_Security_Breaches_Empirical_Evidence_from_the_Stock_Market
Quantifying the Financial Impact of IT Security Breaches: What Do Investors Think? (2003)	Firms affected by a cyber breach experienced a 2.7% decline in their stock price relative to the overall market on the day following the attack.	Event Study Methodology	Garg, Curtis & Halper	https://www.emerald.com/insight/content/doi/10.1108/09685220310468646/full/html
The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers (2004)	Firm announcements of internet security breaches are negatively associated with stock market level. Additionally, the market value of security developers increases due to security breach announcements. Though security breaches negatively impact all firms, breaches are particularly damaging to smaller firms' survivability.	Breach announcements from Lexis/Nexis database, CNET and ZDNET. Stock return data came from the Center for Research in Security Prices (CRSP) database.	Cavusoglu, Mishra & Raghunathan	https://pdfs.semanticscholar.org/5d52/2df06172a015d0b6cb5e86b9aa4d2697280b.pdf?_ga=2.234778782.1238268202.1565976421-1152664833.1565976421
Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms (2009)	Breaches affecting information confidentiality and availability have long-term negative impacts on company stocks. However, firms may also invest in security after a breach, which can lead to long-term economic benefits. Breaches involving information integrity may experience immediate negative stock	*Matched sampling* methodology used to explore impact of each type of breach, IT intensity and size. Business news articles from Lexis/Nexis Academic database. Compustat used to filter	Ko, Osei-Bryson & Dorantes	https://www.researchgate.net/publication/220065342_The_Economic_Cost_of_Publicly_Announced_Information_Security_Breaches_Empirical_Evidence_from_the_Stock_Market

	reactions, but the damage does not persist in the long-run.	out cases with missing financial data.		
A multi-level approach to understanding the impact of cyber crime on the financial sector (2014)	Important factors in determining the costs of cyber crime include: shifts in strategic priorities and, having as key objectives, protection of customer trust/loyalty and market positioning vis-a-vis competitors. Effective strategies to protect a company's business interests and market positioning in the event of cyber crime can minimize the costs of the attack.	Data on cyber attack costs collected through surveys and interviews with industry representatives across sub-sectors: banking, cards, insurance, retail, online payment providers, financial services and government fraud service. Used system dynamics (SD) methodology to build a causal loop diagram (CLD).	Lagazio, Sherif & Cushman	https://core.ac.uk/download/pdf/20543077.pdf
Financial and non-financial implications of cybercrimes in emerging countries (2015)	Non-financial impacts of cyber crime include loss of customer confidence, negative publicity, diminishing productivity, business discontinuity, loss of confidential customer or company data, unauthorized access to certain product innovations, loss of intellectual property, and more. While these costs are difficult to quantitatively measure, their impact is certainly significant.	N/A	Antonescu & Birau	https://core.ac.uk/download/pdf/82376169.pdf

Beneath the surface of a cyberattack: A deeper look at business impacts (2016)	External impacts may only account for a small percentage of the overall breach cost. Value of lost contract revenue, devaluation of trade name and lost value of customer relationships made up nearly 89% of the financial costs. Cyber attack impacts continue to pervade companies years after the attack.	Discounted Cash Flow Method under the Income Approach (future value of an asset), "With-and-without" method (estimating value of an asset with and without cyber attack occurrence), "Relief-from-royalty" method (devaluation of trade name). Zurich Insurance for average costs of customer breach notification/protection.	Deloitte	https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf
Analysis: How data breaches affect stock market share prices (2018 update)	In the long-term, companies that were breached underperformed the market. Finance and payment sectors saw the greatest reductions, while the healthcare sector was least affected.	Difference in % Share Price before and after breach vs NASDAQ, all 24 companies publicly listed on NYSE.	Bischoff	https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/

B. Studies that found long-term stock reduction *amplified in the financial sector*

Title	Summary	Data	Author(s)	Source
How does cyber crime affect firms? The effect of information security breaches on stock returns (2017)	There is a significant overall negative market reaction to announcements of security breaches. The reaction is significant across both financial and non-financial firms, but the negative impact is greater amongst firms in the financial sector. In the financial sector, there is a negative market reaction to firms prior to the announcement of the attack, suggesting that the attackers are involved in insider trading.	Newspaper reports on cyber attacks between 1995-2015. Obtained stock market prices (adjusted for dividends and splits) from Datastream database.	Arcuri, Brogi & Gandolfi	http://ceur-ws.org/Vol-1816/paper-18.pdf
Impact of Cyberattacks on Stock Performance: A Comparative Study (2018)	Markets do not react significantly to cyber attacks. Firm reactions to cyber attacks are also not significant for the industrial, information technology, and health sectors. In the financial sector, there is strong evidence of firm reaction in the short-term, but the effects dissipate long-term.	Event Study Methodology (ESM). Uses data breach announcement information of firms listed on S&P 500. Breach Level Index (BLI) used to establish public announcement dates for breaches of recorded firms.	Twenebo ah-Koduah, Atsu & Buchana n	https://www.researchgate.net/publication/326440549_Impact_of_Cyberattacks_on_Stock_Performance_A_Comparative_Study
What is the impact of successful cyberattacks on target firms? (2018)	Firms that suffer attacks on customers' personal financial information experience equity value losses $1.06 billion greater than breaches not involving personal financial information.	Identified data breaches using PRC (Privacy Rights Clearinghouse) database. Matched firm names from PRC database with Compustat and CRSP database to find stock information. Checked Capital IQ and Factiva for firm name accuracy if firm not in Compustat or CRSP. Sample firms must	Kamiya, Kang, Kim, Milidonis & Stulz	https://www.nber.org/papers/w24409.pdf

		be listed on New York Stock Exchange, American Stock Exchange and NASDAQ.		

C. Studies that found NO significant stock impact

Title	Summary	Data	Author(s)	Source
The Impact of Virus Attack Announcements on the Market Value of Firms (2004)	Markets do not penalize firms affected by cybersecurity breaches, resulting in a lack of incentive for managers to develop security	Searched Lexis-Nexis database for business news articles. Used Center for Research in Security Prices (CRSP) database to find stock market information for firms.	Hovav & D'Arcy	https://www.researchgate.net/publication/220449894_The_Impact_of_Virus_Attack_Announcements_on_the_Market_Value_of_Firms
The Impact of Information Security Breaches Has There Been a Downward Shift in Costs (2011)	News reports on information security breaches have significant impact on the stock returns of firms. Breaches that affect information availability also have significant negative impact on stock returns of firms. In recent years, the attitude toward breaches seems to have shifted towards that of a nuisance as opposed to an economic threat. The researchers fear that this attitude will result in neglected risk management issues in firms' critical digital infrastructure, which can present national security implications.	Search of Financial Times, New York Times, USA Today, The Wall Street Journal and The Washington Post. Sites chosen because of their high investor following. Used CRSP database to identify stock market information of firms.	Gordon, Loeb & Zhou	https://www.researchgate.net/publication/220065392_The_Impact_of_Information_Security_Breaches_Has_There_Been_a_Downward_Shift_in_Costs
Why Data Breaches Don't Hurt Stock Prices (2015)	Companies do not see stock impact after cyber breach, and may even see increases in earnings. Shareholders do not have any good metrics for measuring business implications of cyber attacks, so stocks do not see much impact.	Looks at several recent breaches: Home Depot, Target, Sony, Sears, and JP Morgan Chase	Kvochko & Pant	https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices