RESEARCH MEMO

FDD | CCTI Center on Cyber and Technology Innovation

Any Publicity is Good Publicity? Data Breaches and Firm Reputation

By Christos A. Makridis

June 3, 2020

Corporate data breaches have risen over the past 15 years,[1] with spectacular mega-breaches increasingly frequent and common.[2] However, it is not clear how these breaches exact an economic consequence on the affected firms,[3] aside from legal costs in the aftermath. Economic research has produced ambiguous estimates of how data breaches affect these firms' share prices.[4] One might even infer that based on shareholder response (or lack thereof), capital markets care little about corporate data protection.

Original research presented here shows how publicly reported data breaches can actually improve the reputations of firms.[5] Looking at a sample of 43 firms, brand power and familiarity actually *increase* by 13 to 22 percent following an average-sized data breach. However, the costs appear to go up with the size of the breach. Indeed, in the aftermath of 11 of the largest data breaches assessed, brand power and familiarity *decrease* by 14 to 18 percent.

The Research

The economics research community is only in the early stages of understanding the effect of data breaches and malicious cyber incidents on shareholder value. But the implications are significant for regulatory policy. If companies do not suffer consequences for cyber incidents, then they will have no reason to make more than a minimal investment to protect the data of their stakeholders (customers, employees, suppliers, et cetera). At present, publicly held companies do not appear to pay a steep price.[6]

1. The White House, "Economic Report of the President," March 2019. (https://www.whitehouse.gov/wp-content/uploads/2019/03/ERP-2019.pdf)
2. Benjamin Edwards, Steven Hofmeyr, and Stephanie Forrest, "Hype and heavy tails: A closer look at data breaches," *Journal of Cybersecurity*, Volume 2, No. 1, December 30, 2016, pages 3-14. (https://academic.oup.com/cybersecurity/article/2/1/3/2736315)
3. Sasha Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, Volume 2, No. 2, December 2016, pages 121-135. (https://academic.oup.com/cybersecurity/article/2/2/121/2525524)
4. Georgios Spanos and Lefteris Angelis, "The impact of information security events to the stock market: A systematic literature review," *Computers & Security*, Vol. 58, Issue C, May 2016, pages 216-229. (https://dl.acm.org/doi/10.1016/j.cose.2015.12.006)
5. Christos Makridis, "Do Data Breaches Damage Reputation? Evidence from 43 Companies Between 2002 and 2018," SSRN Working Paper, May 9, 2020. (https://hq.ssrn.com/submissions/MyPapers.cfm?partid=2056105&redirectFrom=true)
6. Georgios Spanos and Lefteris Angelis, "The impact of information security events to the stock market: A systematic literature review," *Computers & Security*, Vol. 58, Issue C, May 2016, pages 216-229. (https://dl.acm.org/doi/10.1016/j.cose.2015.12.006); Christos Makridis and Benjamin Dean, "Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities," *Journal of Economic and Social Measurement*, Vol. 43, No. 1-2, 2018, pages 59-83. (https://content.iospress.com/journals/journal-of-economic-and-social-measurement/43/1-2)

Christos Makridis is a visiting fellow at the Foundation for Defense of Democracies (FDD), where he contributes to FDD's Center on Cyber and Technology Innovation (CCTI). He is a research professor at Arizona State University and a non-resident fellow at MIT Sloan's Initiative on the Digital Economy and Harvard Kennedy School's Cyber Security Project.

The methodology for this research consists of several layers. First, it draws from related literature on the economic effects of information technology and security investments on firm value.[7] Next, to understand how publicly reported data breaches affect firm reputation, this research utilizes the CoreBrand Index from Tenet Partners, which measures several dimensions of a company's reputation at a quarterly frequency across 1,000 companies since 2001 (and annually since 1990). The CoreBrand Index is constructed from survey responses among business executives (i.e., the level of vice president and above) across major corporations to assess a combination of "familiarity" and "favorability," where favorability is a function of "overall reputation," "perception of management," and "investment potential" ratings. Overall, the index captures sentiment among informed individuals in the marketplace about specific companies.[8]

This research focuses on two specific inputs of the CoreBrand Index – brand power and familiarity – before and after a data breach. To account for the possibility that a firm may experience a data breach when its reputation is already performing poorly – for example, if a company experiences a decline for other reasons and has fewer resources to devote to information security – firm performance (e.g., revenue) is included as a control. Drawing data from a cohort of publicly traded companies and controlling for firm revenue, employment, and capital, this research finds that brand power and familiarity increase by 22 percent and 13 percent, respectively, following a data breach.

These increases, rather than decreases, in firm reputation following a data breach may seem counterintuitive given the conventional view that negative publicity hurts brand value and firm performance. But the evidence shows that negative publicity can have positive effects.[9] For example, negative press can actually elevate a firm's public profile

7. Chai, Sangmi, Kim, Minkyun, and Rao, H. Raghav, "Firms' information security investment decisions: Stock market evidence of investors' behavior," *Decision Support Systems*, Vol. 50, No. 4, March 2011, pages 651-661. (https://www.sciencedirect.com/science/article/pii/S0167923610001417); Feng Xu, Xin (Robert) Luo, Hongyun Zhang, Shan Liu, and Wei (Wayne) Huang, "Do Strategy and Timing in IT Security Investments Matter? An Empirical Investigation of the Alignment Effect," *Information Systems Frontiers*, Vol. 21, No. 5, October 2019, pages 1069-1083. (https://ideas.repec.org/a/spr/infosf/v21y2019i5d10.1007_s10796-017-9807-6.html); Indranil Bose and Alvin Chun Man Leung, "The impact of adoption of identity theft countermeasures on firm value," *Decision Support Systems*, Vol. 55, No. 3, June 2013, pages 753-763. (https://www.sciencedirect.com/science/article/pii/S016792361300081X); Jason K. Deane, David M. Goldberg, Terry R. Rakes, and Loren P. Rees, "The effect of information security certification announcements on the market value of the firm," *Information Technology and Management*, Vol. 20, January 1, 2019, pages 107-121. (https://link.springer.com/article/10.1007/s10799-018-00297-3)

8. The familiarity index is a weighted percentage of survey respondents who are familiar with the corporate brand, which is rated on a five-point scale. The favorability index is an average of the three attribute ratings (overall reputation, perception of management, and investment potential), which are each rated on a four-point scale. Although this sample of respondents is not representative of consumers, these business leaders reflect the investment community, business patterns, and business customers across major industries. The survey audience is refreshed each year and randomized based on "a proprietary list of influential consumers and qualified business decision-makers," serving as "impartial observers" in that they are both "knowledgeable consumers and business decision-makers." See page 82 of the following for more discussion of the sample characteristics: James Russell Gregory, "Intangible Capital: Culture of Innovation and Its Impact on the Cash Flow Multiple," *University of South Florida*, PhD Dissertation, 2018. (https://core.ac.uk/reader/216960250)

9. Alice M. Tybout, Bobby J. Calder, and Brian Sternthal, "Using Information Processing Theory to Design Marketing Strategies," *Journal of Marketing Research*, Vol. 18, No. 1, February 1, 1981, pages 73-79. (https://journals.sagepub.com/doi/10.1177/002224378101800107); Robert O. Wyatt and David P. Badger, "How Reviews Affect Interest In and Evaluation of Films," *Journalism & Mass Communication Quarterly*, Vol. 61, No. 4, December 1, 1984, pages 874-878. (https://journals.sagepub.com/doi/pdf/10.1177/107769908406100421); Jacob Goldenberg, Barak Libai, Sarit Moldovan, and Eitan Muller, "The NPV of bad news," *International Journal of Research in Marketing*, Vol. 24, No. 3, September 2007), pages 186-200. (https://www.sciencedirect.com/science/article/abs/pii/S0167811607000298); David A. Reinstein and Christopher M. Snyder, "The Influence of Expert Reviews on Consumer Demand for Experience Goods: A Case Study of Movie Critics," *Journal of Industrial Economics*, Vol. 53, No. 1, February 2005, pages 27-51. (https://www.researchgate.net/publication/4992942_The_Influence_of_Expert_Reviews_on_Consumer_Demand_for_Experience_Goods_A_Case_Study_of_Movie_Critics)

if it is not well-known.[10] This is consistent with the old adage, "any publicity is good publicity." Less visible brands can garner positive publicity, even if some of the media coverage is negative.

However, data breaches have a tipping point. When restricting the sample to the largest and most spectacular data breaches, brand power declines by 17 percent and familiarity declines by 16 percent. These estimates are consistent even after controlling for the usual characteristics of a firm, such as employment or revenue. Moreover, when focusing on firms with a larger public profile, there is an even greater decline of 26 percent and 18 percent in brand power and familiarity, respectively. This would indicate that better-known brands are more sensitive to positive and negative media.

Conclusion and Policy Recommendations

Although data breaches have become more common, businesses are not always making the necessary cybersecurity investments to keep pace with the growing danger. While many publicly traded companies are exposed to significant cyber risk,[11] firms may choose to under-invest in their security infrastructure if the economic consequences are not severe.[12] Admittedly, more research is needed, particularly to expand the sample. Still, judging from this sample of large, publicly traded firms, initial assessments show that data breaches do not result in reputational damage. Instead, there are often positive effects arising from media exposure and familiarity.

But the absence of economic consequences has a potentially deleterious effect. Companies have few incentives to invest in cybersecurity. This means more data is at risk. The following recommendations should therefore be considered:

1. **Create a national and harmonized data breach notification law**. While nearly all states now have their own version of data breach notification laws, they may differ in meaningful ways. Because publicly traded companies often operate in some capacity across all U.S. states and territories, the lack of a clear and unified national standard creates uncertainty and fragmentation. This may prevent cybersecurity investments that may otherwise be undertaken. The federal government could establish a minimum standard that individual states could potentially enhance if they so choose, allowing for federalism to prevail. This suggestion parallels the recommendation by the congressionally chartered Cyberspace Solarium Commission to create a national breach notification law that supersedes all existing state and local laws.[13]

2. **Enhance procurement policies for federal contractors and defense companies**. The federal government has significant purchasing power, which it can leverage to improve cybersecurity best practices in the private sector by requiring contractors to maintain a baseline of cybersecurity precautions and performance. While the government should not be in the business of micro-managing, it is reasonable to set performance standards, particularly with defense companies, to ensure improvements across the contractor community. Since supply chains are inherently interconnected, a change in policy for defense companies could generate important ripple effects across other industries.

10. Jonah Berger, Alan T. Sorensen, and Scott J. Rasmussen, "Positive Effects of Negative Publicity: When Negative Reviews Increase Sales," *Marketing Science*, Vol. 29, No. 5, September-October 2010, pages 815-827. (https://www.ssc.wisc.edu/~sorensen/papers/negative_publicity_2010.pdf)
11. The White House, "Economic Report of the President," March 2019. (https://www.whitehouse.gov/wp-content/uploads/2019/03/ERP-2019.pdf)
12. Sasha Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, Volume 2, No. 2, December 2016, pages 121-135. (https://academic.oup.com/cybersecurity/article/2/2/121/2525524)
13. Senator Angus King and Congressman Michael Gallagher, Cyberspace Solarium Commission, Final Report, March 2020. (https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view)

3. **Maintain a secure national database of malicious cyber incidents for research**. While several existing databases track data breaches and other malicious cyber incidents, the data are insufficient for serious research that can benefit U.S. businesses. Current data either omit firm names or overlook certain malicious cyber incidents, making it tough to build predictive models that relate malicious attacks with financial outcomes. The National Cyber Investigative Joint Task Force already has a strong record in working to "coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation."[14] This successful interagency structure could provide a model for securely sharing data on malicious cyber incidents, including granular information about both the exposed firm and the attacker.[15]

The trendline of corporate breaches indicates that the problem is likely to grow worse. But the limited or even positive impact of breaches suggests that companies may not be sufficiently motivated to protect their data. These recommendations can help guide the private sector toward a safer future and allow the federal and state governments to lead the way.

14. Federal Bureau of Investigation, "National Cyber Investigative Joint Task Force," accessed June 2, 2020. (https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force)

15. The Securities and Exchange Commission already makes available data on financial misconduct at a firm-level through its Accounting and Auditing Enforcement Releases, so similar information on data breaches would be a natural extension for compliance.