HACKING INDUCED EXTERNALITIES AND THE APATHY OF STOCKHOLDERS

Marina Azzimonti and Asher Marks

1. Introduction

With some of the largest companies in the United States suffering from cyber intrusions, the economic impact of these attacks comes into question. As of date, there is very little information regarding how much hacks cost to companies and whether they have a significant economic impact. In this paper, we study the effects of a hack in the stock price of publicly traded firms in a short window around the event, as well as on the company's reported quarterly revenues. We find that, on average, the stock price falls by 3.5% upon impact, and recovers quickly (after a day). Quarterly revenues are mostly unaffected. This may seem surprising, given the large number of records lost in our sample (no less than 100,000) and the average cost of class action suits incurred by hacked companies. The explanation lies on the fact that most companies have "cyber insurance", which mitigates the impact of an intrusion and even pays the legal fees once the company gets sued in a class action suit. Because companies are only partially liable for the loss of their consumers' records, the price of the hack is actually greater then what the company is held accountable for. The resulting externality is not taken into account by the company when investing on technology to prevent the hacks. We end the paper by discussing potential measures that could be undertaken by the government to resolve this inefficiency.

To date, very few researchers have analyzed the effect of intrusions on a company's revenue. Goel and Shawky (2009) studied the fluctuation of stock prices of

publicly traded companies to look for patterns caused by a hack[1]. The IEEE (2011) focused on the announcement of software vulnerabilities and the relation of the announcement to the firm's market price. Gordon, Loeb, Lucyshyn, and Zhou (2015) performed a cost-benefit analysis of information security investments. Bauera and van Eetenb (2009) formalized the nature of the externality in a theoretical model.

2. What is Hacking?

President Obama made a statement after the Sony hack in 2014 calling the cyber threat "one of the most serious and economic and national security challenges we face as a nation." Over the past decade, malicious cyber intrusions have become the biggest source of credit card and identity fraud. With over 760,000-recorded hacks since 2005, companies and governments are struggling to formulate methods for which to detect and prevent cyber hacking with the hopes of mitigating potential fallout for the effected consumer.

The most effective cyber intrusion technique is called "Spear Phishing." The hacker sends a legitimate looking email to thousands of recipients with the hopes of one recipient opening the email. Once the email and/or attachment is opened, malware is spread throughout the targeted system and the hacker gains access to restricted data. Hackers typically use an infected computer to spread the virus to the entire system by embedding the code into the servers and igniting a ripple effect [2]. This technique was put to the test against Google in 2014, which resulted in the largest data breach in Google's history.

[1] See also Garg, Curtis, and Halper (2003)
[2] http://www.cnbc.com/id/48087514/page/1

3. Empirical Analysis

3.1 Data

The database is constructed for the period 2005-2015. We obtained the list of hacked companies using an online database created by Privacy Rights Clearinghouse[3]. The initial list, which contains 760,000 hacks, was narrowed down according to the following criteria:

i. Only publicly traded companies who suffered hacks with more than 100,000 records lost were considered.

ii. We focused on "All Hacking or Malware Attacks" of businesses and healthcare companies since 2005[4].

iii. Data breaches had to be caused by intentional hacking by a third party.

Focusing on data breaches caused by intentional hacking by a third party, the data set can be narrowed down to 750 hacks in the last ten years. We restricted the sample consider to publicly traded companies because the Securities and Exchange Commission requires all publicly traded companies to release quarterly and annual financial reports including stock prices and unexpected expenses. Due to the availability of this vital information, only publicly traded companies in the United States could be accurately analyzed. The limit of data loss greater than 100,000 records was set as any smaller amount would be unquantifiable using financial modeling. Overall, only 33 companies in the last ten years

[3] "Privacy Rights Clearinghouse." N.p., n.d. Web. 08 May 2016.
[4] http://www.privacyrights.org/data-breach

had data losses greater than 100,000 records, were publicly traded domestically, and reported the cyber intrusion to the public.

The historical stock quotes of the 33-targeted companies were extracted from 'Yahoo Finance!' for a window around the event. The "date of the hack" is defined as the date in which the hack was made public. We use this date because we are interested in the effect on its stock market price is considered was used to pull the stock prices and volume of shares traded for the timeframe of the hack. Due to the short-term nature of the hack, stock information was gathered for three business days before the intrusion, the day the intrusion was made public, and then three days post intrusion.

3.2 Prominent hacks and Event Study

In 2009, Heartland Payment Systems suffered a large cyberattack in which 130 million credit card records were stolen. The Federal Bureau of Investigation ruled that they could not locate the perpetrators. Their stock price dropped 39.7% the day after the hack, and increased to a 75% drop three months later[5]. Estimated expenses from the intrusion were $12.6 million.

Surprisingly, most companies *do not* suffer important decreases in stock prices once their cyber breach is announced. In 2013, the Associated Press's (AP) Twitter account was hacked. The AP's stock dropped 0.88% in an hour but leveled off with the price pre-hack soon after. In 2015, Anthem Insurance Corporation was hacked resulting in the loss of 80 million records containing social security numbers, addresses, date of

[5] http://www.bloomberg.com/bw/stories/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice. Also see Armerding (2016)

births, medical history records, and other sensitive information. This hack was the largest in 2015, but the pattern was similar. On the date of the hack, the stock fell from $136.65 to $135.11. Two days after the hack, the stock price fell to $134.31, a total loss of 1.7%. Three days after the hack, prices rose to 1.09% above pre-attack prices.

The biggest hack in recorded history occurred in 2013 when Adobe Systems was hacked leading to 152 million records. The stock price drop for the largest hack in history was only 3.8%.

To analyze this more systematically, we performed an event study by computing the average decline in stock prices for our sample in a three-day window around the hack. The result is depicted in Figure 2. Consistently with the descriptive analysis above, we find that when all hacked companies are considered, the average decline in stock prices is small, around 3.5%.

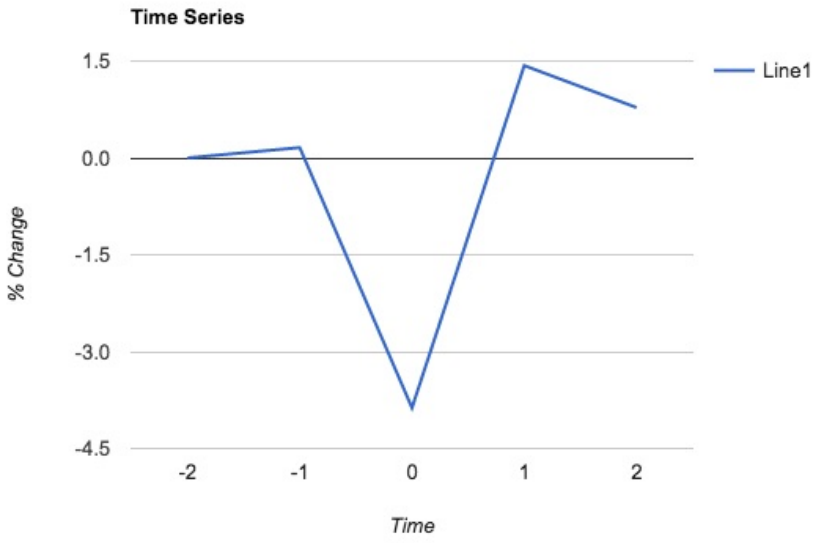

Figure 1: Event Study (date of the hack indicated by time=0)

With the exception of Heartland Payment Systems's hack, we find that the effect of cyber-attacks in stock prices is negligible and incredibly short-lived. This raises the

question of why has the public sector become apathetic to hacks. The answer lies on the fact that soon after Heartland Payment Systems's cyberattack, companies began to invest in *cyber insurance*. This new investment has mitigated damage and reduced the average price drop to less than 3%.

4. How are firms reacting to cyber-attacks?

Companies are doing very little to counteract the threat of cyber intrusions. JP Morgan spends $2.5 billion on cyber security, which is less than 2% of their annual revenue. In 2013[6], insurance companies spent $684 per employee in cyber protection and information security. The largest hacks have targeted financial institutions and those firms only spend $553 per employee. It is interesting to note that firms find it more cost effective to cover expenses related to a hack occurred rather than investing on preventing it. Because much of these costs are covered by cyber insurance, investors do not suffer loses on dividends or observe large effects on profits. A medium sized financial company like Brown Brothers pays a little over a million dollars a year in exchange for $50 million worth of insurance coverage. The fee for the insurance is filed as an average expense and therefore protects them from a financial blowback if hacked.

It is estimated that JP Morgan's large cyber intrusion in 2013 costed $110 million. This price tag includes lawyer fees from litigation and the price of fixing the issue. If the company had to pay that bill, the stocks would have been significantly affected and would have taken months to recover. However, JP Morgan pays over $5 million a year in cyber insurance, which buys about $100 million coverage. As a result, the company paid

[6] http://www.wsj.com/articles/financial-firms-bolster-cybersecurity-budgets-1416182536

about $10 million for the hack, which is less than 0.05% of their revenue. This very low price tag implies that a hack does not impose a significant enough expense shock for investors to care.

When analyzing the effects of hacks into quarterly revenues of companies in our sample, we find basically no difference between the quarter of the hack and a window around the event (details omitted, but available upon request). The reason being that the price of insurance is included as a normal expense, and as long as the company reports being hacked, it does o not incur additional fines from government regulators. Hacked companies, therefore, do not suffer unexpected expenses due to the hack.

Government Policies

The New York State Department of Finance and the federal Office of the Comptroller of the Currency took steps in 2014 to deal with cyber intrusions. Both organizations are requiring publicly traded companies to purchase cyber insurance. The hope is that by having insurance, companies can plan for the annual expense and therefore will not result in layoffs or stock decreases if hacked and uninsured.[7] The problem with this approach is that the insurance protects the company's interests but not the interests of the consumers whose records are stolen.

Requiring spending on cyber defense would protect consumers as well, by making companies internalize the externality of records lost. Alternatively, stating that companies cannot pay legal fees and government fines with insurance money could motivate companies to mitigate the risk and increases cyber security defenses.

5. Conclusion

[7] See Bolot and Lelarge (2009) for an interesting environment in which by forcing companies to buy insurance, they have incentives to invest in preventing cyber-risks as well.

Cyber intrusions are becoming the biggest threat to companies in the modern era. With the average hack costing over $16 million each, cyber insurance has become a fixed expense, reducing the incentive of firms to invest on preventing cyber-attacks.

The negative externality caused by hacks could be remedied through government intervention. Policies requiring increased information security prevention services needs to be implemented in order to effectively protect the consumer.

References

Armerding, Taylor (2016). "The 15 Worst Data Security Breaches of the 21st Century." CSO Online. N.p., 15.

Bauera, Johannes M. and Michel J.G. van Eetenb (2009) “Cybersecurity: Stakeholder incentives, externalities, and policy options,” Telecommunications Policy, Volume 33, Issues 10–11.

Bolot, Jean and Marc Lelarge (2009) "Cyber Insurance as an Incentive for Internet Security," Managing Information Risk and the Economics of Security. Springer.

Garg, Ashish, Jeffrey Curtis, and Hilary Halper (2003) "Quantifying the financial impact of IT security breaches", Information Management & Computer Security, Volume 11, Issue 2.

Goel, Sanjay and Hany A. Shawky (2009) "Estimating the Market Impact of Security Breach Announcements on Firm Values." Information & Management, Volume 46, Issue 7.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou (2015) “Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model,” Journal of Information Security, Volume 6 Number 1.

Verizon (2016) “2016 Data Breach Investigations Report: It’s back, and it’s more insightful than ever.” Available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/