THE EFFECT OF DATA BREACHES ON SHARE PRICES

A dissertation
Submitted to
the Temple University Graduate Board

In Partial Fulfillment
of the Requirements for the Degree
DOCTORATE IN BUSINESS ADMINISTRATION

---

by
Michael Thomas McGarry
Diploma Date May 2022

Dr. Min-Seok Pang, Advisory Chair, Management of Information Systems, Temple University
Dr. Lynne Andersson, Department of Human Resource Management, Temple University
Dr. Elizabeth Gordon, Department of Accounting, Temple University
Dr. David Lanter, Department of Management Information Systems, Temple University
Dr. Lalitha Naveen, Department of Finance, Temple University

ABSTRACT

Data breaches are the theft of sensitive information or the disruption of company operations through cybercriminal acts. This paper studies the impact data breaches have on stock prices. I use the findings to make a public policy recommendation which I believe will facilitate future cybersecurity improvements.

The impact of a data breach on stock prices is not well understood. The existing research is contradictory: Some research has found that a data breach has a statistically significant, long-term, negative impact on stock price. Others have found that data breaches have no impact. One study found a statistically significant negative impact but that the share price quickly recovers (Richardson et al., 2019). Share price reflects the market's consensus option of the value of a firm. Clarity on the impact of a data breach on share price would help companies establish an appropriate cybersecurity investment strategy. The lack of clarity in the research makes establishing a strategy difficult.

This paper studied the share price movement of companies who disclosed a data breach between January 2007 and September 2020. It found, through event studies and statistical tests, that data breaches have a statistically significant negative impact on share price. These results were heavily influenced by a few extreme cases.

Interviews with research analysts and investors found that they regard data breaches as immaterial. They do not believe customer behavior changes as a result of a breach. They also do not believe that the cost of a breach is material to a financially sound company.

The implication is that companies should be wary of over-investing in cybersecurity. Company strategy should be to do what is necessary for regulatory compliance and to be consistent with standard practices.

Market participants suffer from a lack of information. There is not a data source which can be used to determine the probability and cost of a future breach; nor is there a data source to gauge the effectiveness of a security control. Cybersecurity insurers are the natural collection and dissemination point for this data, but they view this information as their source for competitive advantage. They will not willingly share the information. The government should intervene by making the disclosure of breach information mandatory, and then ensuring that this information is widely available.

ACKNOWLEDGEMENTS

I would like to thank my advisor, Dr. Min-Seok Pang, for his guidance, patience constructive criticism, and mentorship.

I would like to thank Doctors Andersson, Gordon and Naveen for being on my committee and their constructive comments throughout the process.

I would like to thank my family, especially my wife Michele, for her patience and support.

Finally, I would like to express my deepest appreciation and love to my parents for their inspiration, installation of a strong belief in the value of education, and their unrelenting support while I was growing up.

TABLE OF CONTENTS

Page

LIST OF TABLES

Table Page

LIST OF EXHIBITS

THE CHANGE IN STOCK PRICE AFTER A DATA BREACH

Introduction

Data breaches, defined as the unauthorized access to confidential information or the disruption of company operations due to cybercriminal acts, have become ubiquitous. Confidential information stolen by criminals includes personal financial information (such as credit card numbers and banking information), intellectual property (the 2014 Sony breach included the theft of four previously unreleased movies), personal health information, and personal identity. See Table 3 for the number of data breaches and millions of records lost per year.

Prominent data breaches include Target (2013, 40 million credit card records stolen), Equifax (2017, 143 million US citizen records stolen), Marriott (2018, up to 500 million customer records, including some credit card and passport information), Capital One (2019, 106 million records), and American Medical Collection Agency (2019, 20 million records). The American Medical Collection Agency breach led to the company's bankruptcy (Bloomberg, 2019). The CEOs at Target and Equifax were fired as a result of their data breaches.

All 50 US states have implemented security breach notification laws and the number of US states with mandated minimum IT security standards has doubled since 2016 (National Conference of State Legislatures, 2019). Companies have been increasing their investments in Information Technology (IT) security defenses. The growth in IT security investments is double the growth in overall IT spending (Gartner, 2019). See Table 4 for the worldwide growth in security spending by year.

The number of publicly announced security breaches increased by 17% in 2019, after a sharp drop in 2018 from 2017's record high (see Table 3). The ITRC theorizes that the increase is due

to new disclosure regulations and because of heightened criminal activity (Identity Theft Resource Center, 2020).

The costs of a data breach can be significant (see tables 6 and 7 for the average cost of a data breach). Target reported that a $202 million net cost of its data breach after insurance reimbursements (Stempel & Breach, 2015). The costs included investigations, remediation services, regulatory fines, and legal settlements. Equifax saw its credit rating downgraded as a result of its data breach (Hogal, et al., 2020). A $12.5 billion class-action lawsuit was filed against Marriott hours after its breach was disclosed (Cimpanu, 2018). The lawsuit is still pending.

The costs discussed above does not consider lost sales due reputational damage. One study found that the impact of reputation loss exceeds other data breach costs (Karniya, et al., 2020).

Academics and practitioners theorize that the costs of a data breach will lower a firm's future cash flows and hence the market valuation of a firm. A literature review found that 71% of academic research found a negative, statistically significant relationship between a data breach announcement and share prices (Spanos & Angelis, 2015).

Others are not so sure. They argue that data breaches have become so common that they should be considered a cost of doing business. Recent articles state that the frequency of date breaches has made consumers numb and apathetic to them (Mele, 2018; Chen, 2020). Breaches are expected and should be considered a regular cost of doing business (Kvochko & Pant, 2015), similar to inventory theft in the retail industry.

As a result, they argue that the change in market value due to a due breach is insignificant. Some academic research supports this theory (Schatz & Bashroush, 2016; Richardson, et al.,

2019). A look at stock price movement after high profile breaches generally supports this view (see Table 5, Equifax being an exception).

The contrasting theories and research findings, combined with the dynamic and complex nature of cybersecurity, make it difficult for boards and senior managers to determine an appropriate budget for cybersecurity defense. Firms are at risk of either over or under investing.

The purpose of this research is to help practitioners understand the cost of a cybersecurity breach by measuring the change in firm market value after a public data breach notification. This will help boards, managers and executives determine the appropriate level of IT security investment.

Literature Review

Although information security is a classic topic in IT research, very few studies examine IT security from a business or economic perspective (Eling & Wirfs, 2019).

The existing research on the market value consequences of a data breach is inconsistent and inconclusive. Some studies conclude that a data breach leads to a negative change in market value (e.g. Morse et al., 2011), other studies did not see a statistically significant change (e.g. Goldstein et al., 2011). One study found a short-term decrease in market value, but the decrease was minor and of short duration (Richardson et al., 2019).

Previous research has shown that investors' ability to predict stock market moves in response to events improves over time (Mikhail, et al., 1997). Cybersecurity and data breaches have been studied for about 20 years. One explanation is that the early studies were plagued by inconsistent market reactions as investors became familiar with data breach effects. Current research could be more consistent as the enhanced familiarity stabilizes investor expectations.

However, this does not appear to be the case, as recent studies have come to differing conclusions (Schatz & Bashroush, 2016; Richardson, et al., 2019; Hogal, et al. 2020).

See Table 1 for sample research concerning IT security and general business impact. Table 2 provides a summary of the research on the relationship between IT security events and a firm's market value.

Cybersecurity is a dynamic and rapidly evolving space; the nature of attacks and the sophistication of the attackers is changing rapidly. Relatively new attacks, such as ransomware, quickly become commonplace. New cybersecurity research is needed to provide clarity to practitioners and academics.

This dissertation will help practitioners by providing evidence of a data breach's impact on market valuation and providing insights into the factors that influence the magnitude of the change in valuation. A better understanding of the impact of a data breach will help guide practitioners making investment and governance decisions.

Conceptual – Relevant Theory

The hypotheses for this research proposal are based upon Institutional Theory, and the Resource-based View of the Firm.

Institutional Theory

Institutional theory describes how management practices and organization structures adapt to social norms even when adaption comes at the expense of organization goals, such as profitability (Meyer & Rowan, 1977).

Society places pressure on organizations to conform to social norms through three institutional forces: 1) Regulatory (laws, monitoring, and enforcement) 2) Normative (social norms, expected behaviors) and 3) Cognitive (Models, congruence with the cultural

environment) (Bruton, et al., 2010). Organizations which do comply are allowed to operate and access societal resources such as shared infrastructure, customers, and employees (Suchman, 1995).

Organizations which do not comply risk having its conduct questioned (Oliver, 1991). For example, Equifax's CEO had to testify before Congress as a result of its data breach (Newman, 2017). Severe non-compliance will place the organization's right to exist at risk (Deegan, 2002).

Organizations which process sensitive information, such as personal financial data, are expected to protect the data. Society codifies and implements this expectation through regulations. The regulations will specify the standards, the oversight process, and the punishments for non-conformance.

Resource-based Theory

The Resource-Based View of the firm argues that the ownership of strategic resources positions a firm for sustained competitive advantage and long-term success. Sustained competitive advantage is a value creating strategy which cannot be replicated by competitors (Barney, 1991). Strategic resources which create sustainable competitive advantage are valuable, rare, immobile, difficult to imitate, and non-substitutable (Barney, 1991). A firm can build on these strategic resources to consistently superior financial performance over time. Examples are well-known and respected brand names, such as Apple or Coca-Cola. The resource-based theory has been widely confirmed in empirical studies (Wade & Huland, 2004).

Extant research has found that IT capability is positively related to a firm's market value (Bharadwaj, 2000; Samburthy, et al., 2003). The stock market has been shown to react positively to IT investment announcements (Bharadwaj et al., 2009). This implies that, consistent with the resource-based view, IT capabilities are a strategic resource.

The converse is that research has established that IT failures have an adverse and material impact on a firm's market value (Bharadwaj, et al., 2009; Goldstein et al., 2011). These failures include operational disruptions due to extended system outages, and unsuccessful projects resulting in cost overruns, write-offs and operational disruptions.

Data breaches are a form of IT failure. They signal to investors that the firm has IT capability deficiencies.

Hypotheses

Additional research is needed on the relationship between data breaches and share price. This relationship has not been fully examined (Eling & Wirfs, 2019), cybersecurity is a dynamic and rapidly evolving field, and the existing research is contradictory (Table 2). My overarching hypothesis, drawing upon Institutional and Resource-Based View theories, is that there is a statistically significant negative relationship between data breaches and share price.

Customers and institutions expect that firms will protect the confidential personal information entrusted to them. Firms which breach this expectation will be punished by customers and societal institutions. The punishment will be seen in reputational damage, lost sales, new litigation, regulatory fines, and increased government oversight.

Customers whose data was stolen by hackers will become dissatisfied and frustrated, and more willing to take their business elsewhere. Potential customers are more likely to choose a competitor. The breached firm will have to offer better terms, such as lower prices, in order to retain existing or attract new customers. The result is that breached firms will see a decrease in future sales.

A firm suffering a data breach can expect punitive institutional actions, such as increased regulatory oversight, enhanced cybersecurity standards, litigation, and fines. Equifax's data breach led to a $700 million fine from the Federal Trade Commission (Whittaker, 2019).

The firm will experience unplanned direct costs as a result of the data breach. The direct costs include the costs to investigate and correct the cause of the breach, expenses for legal and public relations advice, fines, legal settlements, customer notification costs, and the cost of offering remediation services to affected parties (such as free credit monitoring). The firm may be forced to make unanticipated investments to bolster its cybersecurity defenses.

The efficient market hypothesis states that security prices reflect all available public information (Fama, 1970). The hypothesis further states that new information is quickly incorporated into security prices (Malkiel, 2003). The hypothesis has been confirmed through empirical tests (Fama, 1970; Malkiel 2003).

The efficient market hypothesis means that today's change in security prices is the market's reaction to today's news. That is, a change in a firm's security price is a reflection of news concerning the firm, such as macro-economic reports, company announcements, or news effecting the firm's industry.

This means that a change in a firm's share price, immediately after public disclosure, can be attributed to the data breach assuming no other significant firm-specific news and after adjusting for movements in the overall market. The abnormal return is the difference between the actual share price and the expected share price, based upon the change in a market index such as the S&P 500.

Details on calculating abnormal returns are presented in the methodology section.

A firm's market value is the discounted value of future cash flows. The costs and loss in sales caused by the data breach will reduce future cash flows, lowering the market value of the firm. The resulting change in the firm's share price, per the efficient market hypothesis, will occur immediately after the public breach disclosure.

H1: *A data breach will result in statistically significant abnormal negative returns immediately after the breach is made public.*

Data breaches can be classified by the impact and threat they pose to consumers. The loss of personal financial and personal identity information has the highest impact on customers.

Exhibit 1 classifies data breaches by the nature of the breach and the impact to customers. The breach events are listed from lowest to highest impact.

Exhibit 1: Data breach classifications by customer impact

Data breach: Event and the nature of the data lost	**Impact**
Stolen employee information	Low
Operational disruption (example: Ransomware)	Low
Customer contact information (examples: email address, phone #)	Low
Customer login information (username and password)	Low
Personal financial (examples: credit card, bank account numbers)	High
Personal identity (examples: Taxpayer ID, social security number)	High

The loss of personal financial information exposes the customer to monetary loss and financial fraud. The loss of personal identity information exposes the customer to a lifetime of identity theft risk.

Consistent with Institution Theory, the higher impact breaches will lead to more severe penalties from consumers and institutions. Consumers are more likely to take their business elsewhere. Regulatory fines will be higher, for example, the loss of personal health information subjects the breached firm to fines from the Department of Health and Human Services (HHS).

HHS recently increased its fines (HIPPA Journal, 2019). Equifax will pay regulatory fines between $575 and $700 million as a result of its 2017 breach. Banks can sue to recover damages from fraudulent credit card purchases. Target paid $39.4 million in settlements to banks as a result of its 2013 credit card breach (Stemple & Bose, 2015).

Legal costs, regulatory fines, and the unexpected decrease in future sales will lead to a decrease in market value. The decrease in value for a customer's personal information will be greater than the decrease for other types of data breaches.

H2: *The loss in market value will be greater if the data breach includes the loss customer personal information, either financial or identity, relative to other types of data breaches.*

The impact of a data breach will vary by industry.

Depository institutions are based upon consumer trust. Consumers need to be confident that the money given to a bank will be is safe and available when needed. Institution Theory states that an implied social contract exists which specifies that depository institutions will protect the assets given to them. Firms that violate the terms of this contract should expect heavy retributions from Society's Institutions (such as regulatory fines).

Personal information is an asset given to depository institutions. A data breach involving the theft of personal information is a breach of the social contract. The breached firm should expect large regulatory fines, as evidenced in Table 7. Note that financial institutions have the second highest cost per record breached.

Information technology is a strategic resource to business service firms. Unique technical capabilities determine the long-term performance of companies such as Google, Amazon, and Microsoft.

A data breach signals a weakness in technical capability. Technical capability weaknesses are more troubling within technology companies than they are for firms in other industries. The Research Based View of the firm states that this weakness will call into question the firm's ability to compete. Investors lower their long-term financial projections. These revisions will drive the share price down.

The impact of a data breach on depository and technology service institutions will be more pronounced than firms in other industries. We should expect a sharper decrease in their market value.

H3: *Data breaches at depository institutions (SIC major group code 60) and business services firms (SIC major group code 73) will have lower mean cumulative abnormal returns than firms in other industries.*

Cybersecurity insurance minimizes the costs of cyber incidents, such as data breaches, denial of service attacks, and extortion demands. The number of firms with cybersecurity insurance has increased dramatically, from 35% of firms in 2011 to 75% in 2018 (see Table 8).

Cybersecurity insurance typically covers fines, legal fees, remediation services (such as providing credit monitoring services to effected consumers), and data restoration costs.

Cybersecurity insurance minimizes the direct costs of a data breach to firms, protecting a firm's cash flows. The widespread adoption of cybersecurity means, that on average, that the costs of a data breach is lower now than it was at the beginning of the study. We expect that cumulative abnormal returns for breaches disclosed from 2008-2010 to be less than breaches disclosed from 2018 through 2020.

H4: *Firms disclosing a data breach between 2007 and 2010 will have greater cumulative abnormal returns than firms disclosing a data breach between 2017 and 2020.*

Research Methodology

This research will use event studies to determine the effect of a data breach on share price.

Event studies are a generally accepted approach to measuring the effect that an event has on the value of a firm (MacKinlay, 1997). Event studies rely on the rational market hypothesis which states that the impact of an event will be seen immediately in security prices. This enables researchers to measure the effect of a specific event by analyzing the change in share price over a short period of time. Example uses of event studies includes the announcements of mergers and acquisitions, earnings announcements, debt issuances, stock splits, and equity issuances.

Event studies are also consistent past research studying the relationship between data breaches and share prices, as shown in Table 2.

Data sources

Firms included in the research

A sample of data breaches of US publicly traded firms disclosed since January 1 2007.

Publicly disclosed data breaches

The primary data source is the Privacy Rights Clearinghouse (PRC, website https://privacyrights.org/). PRC is a non-profit organization founded in 1992 and dedicated to protecting consumer rights.

PRC provides a database containing information on any event which led to the loss of consumer information, such as sensitive documents found in dumpsters (On Feb 24, 2011 a resident found personal checks and real estate applications in the dumpster behind Prudential Realtors of Hazlewood Missouri); mailing errors (Wells-Fargo of Jacksonville Florida sent bank statements to the wrong customers on October 20, 2011), and data breaches (such as Target's

credit card breach in 2013). Events in the PRC database go back to 2005, and the database can be found at https://privacyrights.org/data-breaches.

The PRC database currently has information on over 9,000 events, including over 6,000 disclosed since 2010. This database has been used in recent academic research (Richardson, et al., 2019; Hogal et al., 2020).

Calculations

This study is based on calculating cumulative abnormal returns over the event window. Abnormal returns are the difference between actual and expected returns.

This approach is consistent with other finance studies, such as a study of the impact of information surprises on share prices (Nimalendran, 1994), political connections (Goldman & So, 2008) and dividend announcements (Damodaran, 1989).

Event window

The event window is based upon the breach disclosure date. This research will use a small event window to help ensure that share price movements are related to the data breach.

Start and end dates are the number of trading days relative to the breach disclosure date. The research is using four event windows

- Start date of -1 (the trading day before the breach was disclosed) to +1 (the trading day after breach disclosure). I included the day before the breach to account for leaks.
- Start date of zero (the day the breach was disclosed), end date of +1 (first trading day after the breach was disclosed)
- Start date of zero, end date of +2 (two trading days after the breach was disclosed)
- Start date of zero, end date of +5 (five trading days after the breach was disclosed)

Expected returns

Expected returns are calculated using the Fama and French plus momentum model (sometimes referred to as the four-factor model). This model extends the Fama and French three factor model, which in turn is an extension of the capital asset pricing model.

The capital asset pricing model calculates expected returns based on the stock's historical return and volatility relative to the market. The formula is:

*RE = RF + Alpha + Beta * (RM -RF)* where:

RE is the expected return

RF is the risk-free rate of return, typically measured using US treasury bonds

Alpha measures a stock's return relative to the rest of the market

Beta measures a stock' sensitivity to overall market changes,

RM is the market rate of return, based upon a market index.

The Fama and French three factor model won a Noble prize in economics for explaining anomalies in stock market returns (Fama & French, 1992). Their research showed that they could explain almost all observed anomalies by adding two factors to the capital asset pricing model. These factors recognize the historically higher returns that small firms and firms with high book to market ratios enjoy. The model is:

*RE = RF +Alpha + Beta * (RM – RF) + (B2 * SMB) + (B3 * HML)*

Where:

RE, RF, Alpha, Beta, and **RM** have the same definitions as in the market model

SMB measures the historic excess returns of small firms relative to big

HML measures the historic excess returns of value stocks.

B2 and **B3** are the betas which reflects the security's sensitivity to the overall market.

Fama and French acknowledged that their model could not explain the positive abnormal returns generated by following a momentum strategy (Fama & French, 1996). Research has shown a momentum strategy generates positive abnormal returns (Jegadees & Timman, 1993). The momentum strategy is to hold, for a short period of time, a portfolio of stocks that has performed well the previous year (or shorting a portfolio of stocks which performed poorly).

This discover of the momentum anomaly led to the three-factor model plus momentum model, whose formula is:

*RE = RF + Alpha + Beta * (RM – RF) + (B2 * SMB) + (B3 * HML)* + (B4 * UMD)

Where:

RE, RF, Beta, RM, B2, B3, SMB and HML have the same definitions as in three factor model

UMD is the market premium for stocks with high recent performance over stocks with lower market performance; **B4** is its beta

Regression parameters

The alpha and the beta values in the models are calculated using linear regression analysis. They are calculated based on actual returns of a maximum 100 trading days, minimum 70, beginning 45 days prior to the start date of the event window. Starting the regression 45 days prior minimizes the likelihood of the event influencing the calculations.

Testing

Hypotheses 1 through 4 will be tested via one-sided t-tests.

The null hypothesis for H1 is that the cumulative abnormal return is zero.

The null hypotheses for H2 through H4 is that there is no difference in the mean values.

Statistical significance is tested using a 95% confidence level.

The t-statistic will be compared to the critical t-statistic for the sample's degrees of freedom.

The t-statistic calculation is:

t-statistic *= Mean / (standard deviation / square root of n)*

Where:

- Mean is the average cumulative abnormal return
- Standard deviation measures the variance in the cumulative abnormal return
- n is the number of data breaches in the sample.

Hypotheses tests

H1 will be supported if the stock price change is negative and statistically significant.

H2 will be supported if:

1. The mean cumulative abnormal return (CAR) for data breaches involving personal financial information and personally identifiable information (breaches classified as high customer impact in Exhibit 1) is negative and statistically significant.
2. The mean CAR for high customer impact data breaches is less than the mean CAR for other types of data breaches.
3. The difference in means is statistically significant.

H3 will be supported if:

1. The CAR for data breaches for firms within the depository institutions and business services industries is negative and statistically significant.
2. The mean CAR for firms within the depository institutions and business services industries is less than the mean for firms in other industries.
3. The difference in means is statistically significant.

H4 will be supported if:

1. The mean CAR for data breaches which occurred from 2007 through 2010 is less than the mean CAR for data breaches which occurred from 2017 through 2020.
2. The difference in means is statistically significant.

Outliers

Potential outliers are defined as data breach events whose abnormal return differs by more than three standard deviations from the data set's mean abnormal return.

The following outliers were excluded from the analysis:

- X-Rite Inc (breach disclosed on April 11, 2012): Danaher Corp announced plans to purchase X-Rite on April 10, 2012.
- Twitter (breach disclosed on June 13, 2016). Microsoft announced on the same day plans to purchase LinkedIn for a 49% premium, driving up share prices of other social media platforms. Twitter's stock went up 8%.
- Cornerstone Brands (ransomware attack disclosed August 11, 2020): Cornerstone announced a 50% increase in earnings per share (EPS) the day the breach was announced. The stock increased by 25% on August 12th.

Data Analysis

The data set consists of 204 data breaches of US publicly traded firms. The breach disclosure dates range from January 12, 2007 to November 28, 2020. The number of breaches by year are shown in Exhibit 2.

Exhibit 2: Number of data breaches in the study by year

Year	Number
2007	8
2008	12

2009	5
2010	13
2011	11
2012	15
2013	14
2014	22
2015	15
2016	22
2017	20
2018	23
2019	7
2020	17
Total	204

The firms in the study represent a number of industries. The number of data breaches in the study by SIC industry code is shown in Exhibit 3.

Exhibit 3: Number of data breaches in the study by SIC major group

Major Group	**Description**	**#**
73	Business Services	48
60	Depository Institutions	23
48	Communications	15
70	Hotels	14
59	Misc Retail	12
63	Insurance Carriers	11
58	Eating and Drinking Places	8
53	General Merchandise Stores	7
45	Air Transportation	5
50	Wholesale Goods	5
67	Investment Offices	5
80	Health Services	5
35	Machinery and Computer Equipment	4
20	Food Products	3
36	Electronic Equipment	3

38	Measurement Devices	3
57	Home Furniture	3
62	Security Brokers	3
79	Recreation Services	3
87	Professional Services	3
15	Building Contractors	2
44	Water Transportation	2
56	Apparel Stores	2
17	Construction Contractors	1
23	Apparel Products	1
26	Paper Products	1
27	Printing Industries	1
28	Chemicals	1
31	Leather Products	1
37	Transportation Equipment	1
42	Motor Transportation	1
47	Transportation Services	1
49	Electric, Gas and Sanitary Services	1
52	Building Materials	1
54	Food Stores	1
55	Automotive dealers/Gas stations	1
61	Credit Institutions	1
78	Motion Pictures	1

There are a surprising number of securities with positive abnormal returns over the event horizon, as shown in Exhibit 4.

Exhibit 4: Negative and positive abnormal returns, by event horizon

Event Horizon	***# Neg***	***# Pos***	***% Neg***
-1 to 1	125	79	61.3%
0 to 2	112	92	54.9%
0 to 1	120	84	58.8%
0 to 5	117	87	57.4%

Test Results

Test of H1: *A data breach will result in statistically significant abnormal negative returns immediately after the breach is made public.*

Figure 1: Test of H1. n=204

Statistical results

Event Window	**-1 to 1**	**0 to +1**	**0 to +2**	**0 to +5**
Mean	-0.52%	-0.51%	-0.71%	-0.92%
Standard Deviation	3.61%	2.96%	4.82%	6.09%
Coefficient of Variation	(6.90)	6.90	6.84	6.43
t-stat	2.07	(2.48)	(2.09)	(2.15)
p-value	**0.02***	**0.01***	**0.02***	**0.02***

** significant using a 95% confidence internal (CI). ** significant using a 99% CI*

H1 is supported across all event horizons, signifying that, on average, a breached firm will suffer a statistically significant decrease in share price.

However, the average impact is small (<1%) across the event horizon. The coefficient of variation is also high, indicating significant variability in stock price impact.

One possible implication is that a few large data breaches may be driving the statistical analysis. The breaches with largest one-day decrease in stock market returns are:

Cumulative abnormal returns, 4 largest one-day decrease in share price

Data breach	**-1 to 1**	**0 to +1**	**0 to +2**	**0 to +5**
Global Payments, 2012	-14.1%	-13.7%	-10.5%	-10.6%
Equifax, 2017	-12.8%	-12.4%	-21.9%	-37.2%
Chegg's, 2018	-13.0%	-13.9%	-13.77	-8.6%
Capital One, 2019	-6.2%	-7.4%	-5.3%	-2.3%

The data breaches were:

- Global Payments lost 1.5 million or more credit cards.
- Equifax lost 143 million customer records. Information lost included social security numbers, taxpayer ids, and driver's license numbers.
- Chegg lost 40 million customer records, including user names and passwords.
- Capital One lost over 100 million credit card applications.

Rerunning the analysis excluding the above data breaches results in:

Event Window	**-1 to 1**	**0 to +1**	**0 to +2**	**0 to +5**
Mean	-0.30%	-0.29%	-0.46%	-0.64%
Standard Deviation	3.25%	2.48%	4.47%	5.51%
Coefficient of Variation	-10.75	-8.64	-9.67	-8.59
t-stat	(1.32)	(1.65)	(1.46)	(1.64)
p-value	0.09	0.05	0.07	0.05

** significant using a 95% confidence internal (CI). ** significant using a 99% CI*

The decrease in share is no longer statistically significant using a one-sided 95% confidence interval.

An analysis of the four largest breaches follows in the discussion section.

Test of H2: *The loss in market value will be greater if the data breach includes the loss customer personal information, either financial or identity, than other types of data breaches.*

Figure 2: Test of H2. CAR after the loss of personal information. n=110

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean	-0.41%	-0.79%	-0.42%	-0.795
Standard deviation	3.66%	5.74%	2.93%	6.75%

t-stat	-1.17	-1.45	-1.52	-1.22
p-value	0.12	0.07	0.06	0.11

Figure 3: Test of H2. CAR for all other breaches. n=94

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean	-0.66%	-0.60%	-0.62%	-1.07%
Standard deviation	3.55%	3.48%	3.00%	5.25%
t-stat	-1.79	-1.68	-1.99	-1.98
p-value	**0.04***	**0.05***	**0.02***	**0.02***

** significant using a 95% confidence internal (CI). ** significant using a 99% CI*

CAR is cumulative abnormal returns

H2 is not supported. The cumulative abnormal returns after data breaches which involve the theft of personal information is not statistically significant, and nor is the cumulative abnormal returns consistently lower than other types of data breaches.

H3: *Data breaches at depository institutions (SIC major group code 60) and business services firms (SIC major group code 73) will have lower mean cumulative abnormal returns than firms in other industries.*

Figure 4: Cumulative abnormal returns for depository institutions, n=23

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean	-0.16%	-0.42%	-0.32%	-0.75%
Standard deviation	2.65%	2.92%	2.44%	3.24%
Standard error	0.55%	0.61%	0.51%	0.68%
t-stat	-0.30	-0.69	-0.63	-1.10
p-value	0.39	0.24	0.27	0.13

Figure 5: Cumulative abnormal returns for business services firms, n=48

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean	-1.42%	-1.88%	-1.01%	-2.34%
Standard deviation	4.09%	7.83%	3.69%	9.14%
Standard error	0.59%	1.13%	0.53%	1.32%
t-stat	-2.40	-1.67	-1.90	-1.77
p-value	**0.01***	0.05	**0.03***	**0.04***

Figure 6: Cumulative abnormal returns for both SIC codes, n=71

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean	-1.01%	-1.41%	-0.79%	-1.82%
Standard deviation	3.71%	6.66%	3.33%	7.75%
Standard error	0.44%	0.79%	0.40%	0.92%
t-stat	-2.29	-1.78	-1.99	-1.98
p-value	**0.01***	**0.04***	**0.02***	**0.02***

** significant using a 95% confidence internal (CI). ** significant using a 99% CI*

The abnormal returns for the two SIC codes are statistically significant. Next, we calculate the means and standard deviations for all other SIC codes.

Figure 7: Cumulative abnormal returns for all other SIC codes, n=133

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean	-0.26%	-0.33%	-0.37%	-0.43%
Standard deviation	3.53%	3.44%	2.74%	4.96%
Standard error	0.31%	0.30%	0.24%	0.43%
t-stat	-0.86	-1.10	-1.54	-1.01
p-value	0.20	0.14	0.06	0.16

The difference between the two independent samples is then tested for statistical significance.

Figure 8: Difference between the two populations

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean difference	-0.75%	-1.08%	-0.42%	-1.39%

Standard error of differences	0.54%	0.84%	0.46%	1.01%
t-stat	-1.39	-1.29	-0.91	-1.38
p-value	0.08	0.10	0.18	0.08

H3 is not supported. The difference in the share price is not significantly different for the event horizons.

H4: *Firms disclosing a data breach between 2007 and 2010 will have greater cumulative abnormal returns than firms disclosing a data breach between 2017 and 2020.*

Figure 9: Cumulative abnormal returns data breaches disclosed between 2007 and 2010, n=38

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean	-0.99%	-1.69%	-0.69%	-2.34%
Standard deviation	3.91%	7.76%	2.32%	8.23%
Standard error	0.63%	1.28%	0.38%	1.34%
t-stat	-1.56	-1.34	-1.84	-1.75
p-value	0.06	0.09	**0.03***	**0.04***

Figure 10: Cumulative abnormal returns data breaches disclosed between 2017 and 2020, n=67

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean	-0.67%	-0.69%	-0.63%	-1.11%
Standard deviation	4.27%	4.73%	3.66%	6.92%
Standard error	0.52%	0.58%	0.45%	0.85%
t-stat	-1.29	-1.18	-1.40	-1.31
p-value	0.10	0.12	0.08	0.10

Figure 11: Difference between the two populations

	-1 to 1	**0 to +2**	**0 to +1**	**0 to +5**
Mean difference	-0.32%	-1.01%	-0.06%	-1.23%
Standard error of differences	0.82%	1.39%	0.58%	1.58%
t-stat	-0.39	-0.73	-0.10	-0.78

p-value	0.35	0.23	0.46	0.22

** significant using a 95% confidence internal (CI). ** significant using a 99% CI*

H4 is not supported. 2007-2010 share prices dropped more than 2017-2020 share prices. However, the decrease in share price is not significant the day after the breach disclosure.

Discussion On The Four Breaches With The Largest Stock Price Impact

Firms disclosing a data breach, on average, suffer a statistically significant decrease in share price. The decrease is not significant if the four largest decreases are excluded. The breaches that led to the four largest percentage decreases in stock price are discussed in the following section.

Methodology

I used a multiple case study approach during this research. The case study is used when the research questions are specified by the researcher prior to the study. They enable researchers to explore the questions and derive insights from real-life events (Benbasat et al., 1987). Data on the four data breaches was collected from secondary sources, such as new stories, investor analysis and academic journals.

The Four Largest Stock Price Drops: Description Of The Events

1. Global Payments (Breach Disclosed On March 30, 2012)

Global Payments provides payment card processing services to merchants, enabling them to accept debit and credit cards. The company processes over 1.5 billion payments annually.

The breach was first reported the morning of March 30th by security blogger Brian Krebs, who wrote that an unnamed company had suffered a massive payment card breach (Krebs, 2012). The Wall Street Journal was the first to name Global Payments (Johnson & Sidel, 2012).

Wired magazine later reported that 10 million payment cards had been stolen during the breach (Zetter, 2012). Global Payments' stock dropped 9% before trading was suspended.

Global Payments did not comment on the breach reports until after the stock market closed. The company confirmed that they suffered a breach of 1.5 million payment cards and scheduled an investor call to discuss the details the following morning.

2. Equifax (Breach Disclosed On September 7, 2017)

Equifax is a consumer credit reporting agency. The company creates credit reports on individuals so that businesses can make consumer lending decisions. Equifax does this by applying a proprietary algorithm to personal data aggregated from external sources of consumer financial information, such as banks, credit card providers, and lenders.

Equifax announced a data breach of 143 million records after the stock market closed on September 7, 2017. The records lost contained highly sensitive personal information, such as social security and driver's license numbers. This type of information cannot be easily changed by those effected by the breach, leading to a persistent identity theft risk to those effected by the breach.

Hackers had taken advantage of a vulnerability within Equifax's web site. The vulnerability was within a widely-used software package created by Apache. Apache announced the vulnerability and released a patch to fit it March 7th, 2017. Apache customers were told that it was a critical vulnerability that could be easily exploited and urged to apply the patch immediately. The Department of Homeland Security contacted Equifax on March 8th and also urged the company to apply the patch. Equifax instructed its IT administrators to apply the patch on March 9th. However, the patch was not applied to the Equifax servers until July 29th after the

security team noticed suspicious network traffic. The web site was taken down the next day (Electronic Privacy Information Center, 2017).

Equifax came under criticism for both the breach, which was viewed as easily preventable, and the company's response. Equifax was criticized for the 6-week gap between breach discovery and breach disclosure. Three Equifax executives sold $1.8 million of stock during this gap, leading to insider-trading investigations by the US Attorney General and the SEC. The web site Equifax created for individuals to determine if they were a victim was riddled with security flaws and logic errors (Krebs, 2017; Rotenberg, 2017). Equifax offered free credit monitoring to victims only if the victim agreed to not participate in class-action lawsuits. Security blogger Brian Krebs called the company's response "haphazard" and "a dumpster fire" (Krebs, 2017). Inc magazine stated that Equifax's inept response made it the worst data breach of all time (Aspan, 2017).

Equifax stock dropped 31% in the 4 trading days after the breach, a market capital loss of $5.4 billion.

3. Chegg (Breach Disclosed On September 25, 2018)

Chegg is an education technology company that provides textbook rentals, tutoring, and other services to students. The company's goal is to disrupt the textbook and tutoring industries by offering middle, high-school, and college students Netflix-style rental services. Chegg was a Wall-Street darling and saw its stock price more than triple since the company's 2013 IPO.

Chegg announced the breach through an 8-K filing. The one-paragraph description stated that Chegg became aware on September 19th of unauthorized third-party access to its customer database starting at or around April 29, 2018. It further stated that the information stolen could

include customer names, shipping addresses, usernames and hashed passwords. The company said that the investigation was on-going.

Chegg stock dropped 12% the day after the 8-K filing. Investors were apprehensive and uncertain; the company did not disclose the size of the breach nor did Chegg's unequivocally state that the breach did not include sensitive information. Investors became concerned that the reputational damage from a large data breach would impact Chegg's future growth (Sharma, 2018).

The breach did result in the loss of 40 million customer records, but the data lost did not include highly sensitive information such as payment cards or social security numbers. Worries that the breach would impact growth were unfounded, as both subscriptions (up 13%) and revenues (up 29%) enjoyed robust growth in the subsequent quarter. The stock price recovered within a month of the breach disclosure.

Capital One (Breach Disclosed On July 29, 2019)

Capital One is a bank holding company specializing in credit cards, auto loans, and banking. It is the third-largest credit card issuer in the United States.

Capital One announced that one of its websites had been breached, leading to the loss of 106 million credit card applications. The information lost included applicant name, address, birthdate, self-reported income, and email address. The breach was executed by an ex-Amazon software engineer (the breaches Capital One web site was hosted at Amazon) who took advantage of a misconfigured firewall and bragged about the data theft on Slack, Twitter and GitHub. The FBI arrested the person the day of the announcement. Capital One management estimated that the breach would cost the company $150 million.

Capital One shares dropped 13.9% in the two weeks after breach disclosure, resulting in a $3.2 billion drop in market value. The stock price recovered to its pre-breach level on November 5th.

Lessons From The Four Largest Events

I. Have a rehearsed, well defined data breach response plan

Research has shown that investors and customers are reassured when a company does not try to minimize the data breach, highlights the security controls that were in place prior to the breach, and then commits to further cybersecurity improvements (Huang and Madnick, 2020).

Neither Global Payments or Chegg had a robust breach communication and response plan. The Global Payment breach was first reported by bloggers and news sources. Chegg announced their breach via a one-paragraph SEC filing. Not owning the communications led to exaggerated media reports based on speculation, hearsay, and rumors. Equifax's response to its breach was heavily criticized (Volz & Shepardson, 2017). Equifax's CEO, who had resigned under duress, blamed the breach on a single IT employee (Lamb, 2017).

Companies should have a rehearsed data breach communications and response strategy. Communications should emphasize that company management takes full responsibility for the data breach, assure stakeholders that the company is taking the breach seriously, describe the security controls that were in place at the time of the breach, and commit to investing in future cybersecurity improvements. If done well, an effective data breach response can minimize the short-term impact on the stock price.

II. Timing can be everything

JP Morgan announced a data breach of one million customer records on August 28, 2014. The number of records stolen was later revised to 83 million, and it still is one of the largest financial-service data breaches of all-time.

The JP Morgan breach is similar to the Capital One's. Both companies are financial institutions, and both breaches led to the loss of tens of millions of customer records. Neither breach resulted in the loss of highly sensitive personal information such as social security numbers, medical history, or payment cards. Capital One executed an effective breach response plan, earning praise from the United States Office of the Comptroller (Barrett, 2020).

Capital One's stock price dropped 13.9% in the two weeks after the breach. The stock took months to recover. JP Morgan's stock was flat after its initial data breach announcement of one million records, and actually went up after announcing that the breach really led to the loss of 83 million records.

Capital One's announcement came one week after the Federal Trade Commission announced a $700 million settlement with Equifax (Schneider & Arnold, 2019). Investors were concerned about potential, Equifax-like, political and regulatory actions (Lambert, 2019). They were skeptical of Management's reassurances that the breach would not impact future earnings (Henry, 2019). One Evermore market analyst wrote:

"*We are skeptical of management's implication that an issue of this magnitude will not impact go-forward earnings and efficiency expectations" (Henry, 2019).*

Capital One, in contrast to Global Payments, Chegg, and Equifax, did everything right when responding to the breach. Unlike Equifax, Capital One did not lose highly sensitive information. Capital One's issue is that its breach announcement came on the heels of the Equifax settlement.

Discussion On Long-Term Stock Price Impact

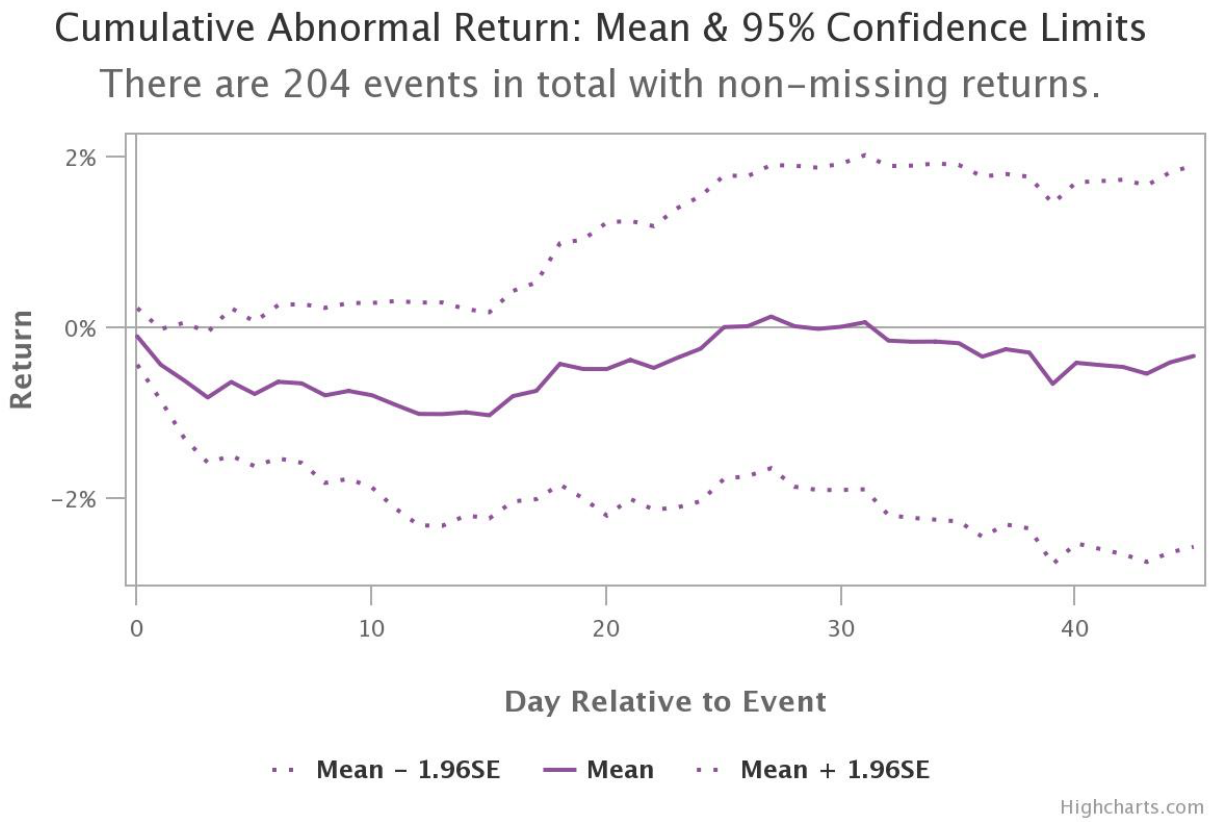
The observed impact of a data breach on stock prices, on average, is <1% across all four event horizons.

The impact does increase with the time horizon, going from -0.51% for (0, 1), to -0.71% for (0, 2) to -0.91% for (0, 5). The decline in share price could be become more significant if the trend continues for a long period of time.

One hypothesis is that investors hold their shares until the details of the breach are fully understood. Investors wait until the costs incurred, such as investments to improve cybersecurity, remediation services, and lawsuits, can be accurately estimated. Investors may wait to trade until they can gauge customer, competitor, supplier, and regulator reactions. The impact of a breach, under this hypothesis, can only be understood by taking a longer-term view of share price performance.

I tested this hypothesis by calculating the mean cumulative abnormal returns up to 45 trading days after breach disclosure, as shown in Figure 12. The graph was created using Wharton Research Data Services.

Figure 12: Longer-term cumulative abnormal returns



The mean cumulative abnormal returns for the 15, 30 and 45 day trading horizons are:

Figure 13: Mean cumulative abnormal returns for longer event horizons

	0 to 15	**0 to 30**	**0 to 45**
Mean	-1.04%	+0.14%	-0.24%
Std deviation	8.81%	13.80%	16.10%
t-stat	-1.68	0.14	-0.21
p-value	**0.05***	0.44	0.42

** significant using a 95% confidence internal (CI). ** significant using a 99% CI*

Other events, such as macro-economic news, competitive actions, and earnings performance, are influencing the longer-term returns. For example, the five largest decreases in share price 45 trading days after disclosure are shown in Figure 14.

Figure 14: Most negative cumulative abnormal returns, 45 trading days after disclosure date

Name	Disclosure date	0 to 1	0 to 5	0 to 15	0 to 30	0 to 45
Carnival Cruise Lines	2020-03-02	-4.8%	-25.1%	-45.2%	-45.9%	-39.8%
Heartland Payment	2009-01-20	-6.8%	-42.7%	-40.8%	-68.3%	-68.9%
Equifax	2017-09-07	-12.4%	-37.2%	-29.1%	-28.4%	-31.9%
MGM Resorts	2020-02-19	+0.43%	-9.7%	-28.7%	-44.6%	-40.3%
Monster.com	2009-01-23	-0.84%	-5.65%	-22.5%	-27.9%	-17.6%

The drop in MGM and Carnival can be attributed to the COVID-19 pandemic. Monster.com was dealing with new competition and a drop in revenue during the 2008-2010 recession.

The data does not indicate that a data breach has a long-term impact. The average stock price recovers (cumulative abnormal return = 0) on the 25th trading day. The change in stock price is not statistically significant at 30 and 45 trading days.

Implications

Wall Street appears to be somewhat indifferent to data breach announcements. While the cumulative abnormal returns are statistically significant, the average is small (<1% on average across the event horizons). And the impact appears to be decreasing overtime, as shown in H4. And H3 shows that the impact is not significant outside of the business service and banking industries.

Future research projects are needed to investigate why the stock price response is muted. Some potential reasons are that companies have minimized the cost of a breach through cyber security insurance, that companies have disclose their cybersecurity risk in SEC filings and the cost of future breaches is already priced into the stock, or, as it is been suggested, consumer

behavior does not change as a result of a breach (Kamula, et al, 2020; Liang & Tabny, 2020; Kvochkol & Pant, 2015). Without a change in consumer behavior, investors will see the cost of a data breach as a one-time event that will not impact future earnings or cash flows.

The implication to companies is that the impact of a data breach, if handled appropriately, is relatively minor. Executives should prioritize minimizing the cost of a future data breach over additional cybersecurity defense investments. Costs can be minimized by transferring risk to third-parties through insurance. Companies should also ensure that breach costs are borne or shared with third-parties when negotiating contracts.

Cybersecurity costs should be minimized, and executives should strive that their firm's defenses are "good enough". This means that firms should be followers, not leaders, in cybersecurity defense. They should be late adopters of new technologies, and the goal should be to implement the minimum necessary to meet regulatory compliance and to be consistent with generally accepted security practices.

HOW INSTITUTIONAL INVESTORS REACT TO A DATA BREACH

My previous chapter analyzed the average stock price change after a data breach announcement. This chapter's intent is to explain the price change by understanding how institutional investors analyze and react to data breach news.

Introduction And Motivation

My previous research found that, on average, companies experience a statistically significant decrease in share price after disclosing a data breach. The decrease is small (< 1%) and is heavily influenced by a small number of events (for example, Equifax's market value dropped 37% in the 5 trading days after its breach). 42% of companies experienced positive abnormal returns in the 5 trading days after disclosure.

These results were counter to my hypotheses. One explanation is that investors view data breaches as one-time events. Previous research has found that one-time events have an insignificant impact on company valuations (Ramakrishnan & Thomas, 1998). But this explanation conflicts with research which found that breached firms experience long-term reputational damage. The reputational damage can lead to decrease in future sales (Karniya, et al., 2020).

The purpose of this research is to understand how institutional investors react to the news of a data breach. Insight into how investors react to a breach will help practitioners set cybersecurity strategy, and contribute to the cybersecurity literature by studying data breaches from an investor's perspective.

Data Collection

Primary data was collected via interviews with regulators, cybersecurity insurers, and cybersecurity insurance brokers. The interviews were semi-structured and approximately one hour in length. The interview participants are summarized below:

Interviewee role	**Number of interviews**
Government/Regulator	5
Cybersecurity Insurer	3
Cybersecurity Insurance Broker	6

The interviewees were asked their opinions on regulatory frameworks, the effectiveness of cybersecurity standards, cybersecurity insurance, and whether institutions had sufficient incentives to invest in cybersecurity.

Secondary data was collected from the interviewees, who often provided internal analysis and assessments. Other data was collected from the academic literature and the practitioner press.

The Efficient Market Hypothesis

I used event studies to analyze stock price movements after a data breach announcement. Event studies rely on the efficient market hypothesis, which states that new public information is immediately reflected in security prices. Studies have found empirical evidence supporting the efficient market hypothesis (Fama 1998; Malkiel, 2003; Boudoukh, et. al., 2012) .

The implication is that the impact of data breaches is immediately reflected in security prices. My research found that a data breach has a minor impact on stock prices. Investor interviews

should confirm that breaches are regarded as immaterial and that they do not influence trading strategy.

Some economists, inspired by behavioral finance, are challenging the efficient market hypothesis. They point out anomalies such as the success of momentum trading. Stocks that have performed well in the past tend to keep out-performing the market, while poorly performing securities tend to continue to under-perform. An investor can realize abnormal returns by buying top-performing securities and shorting poor-performing ones (Fama & French, 1996; Jegadees & Timman, 2001). Researchers theorize that there is a bandwagon effect that draws investors in when stock prices go up or to sell when the market goes down (Cooper and Shiller, 2000; Staumbaugh, Yu, and Yang, 2012). Interviews may find that investors react more to price movements after a data breach than to the news of the breach itself.

There is evidence that investors have a tendency to underreact to new information and that the impact of a news event is only seen over a period of time (Barbens, Shleifer and Vishny, 1997; Kadiyala and Rau, 2002; Savor, 2012). We could find that investors take a "wait and see" approach to data breach news. They hold their positions until they have a full understanding of the event and its economic implications, or, until they see price movement.

My previous chapter did not find that data breaches had a long-term impact on share prices, but that could be distorted because of other events. Interviews could find that investors regard data breaches as significant, but that it takes time for them to fully analyze and react.

Table 9 contains a summary of the extant research on how investors react to news.

Methodology

I used grounded theory as the basis for this research. Grounded theory is an inductive, theory-discovering methodology based upon qualitative data. Theory is discovered through an iterative process of gathering and analyzing data, and then using the data to create and verify theory (O'Reilly, et. al., 2012). This iterative process continues until theoretical saturation is reached, the point in which the researcher believes that additional data gathering will not lead to new information.

Grounded-theory can be used when developing a context-based description of business phenomena (Myers, 2020). It is the appropriate methodology for this study because of grounded theory's focus on context, process, and key actor interpretations (O'Reilly, et. al., 2012).

Data Gathering

Data was gathered via interviews. Interviews are one of the most common and most important data gathering tools within qualitative research (Myers & Newman, 2007).

Interviews were conducted with institutional investors, research analysts, and investor relations managers. The investors and research analysts covered both debt and equity securities. Retail investors, regulators, and consumers were out of scope for this study.

This study used snowball sampling to identify participants. Snowball sampling is a non-probability technique in which existing participants provide references for future interviewees.

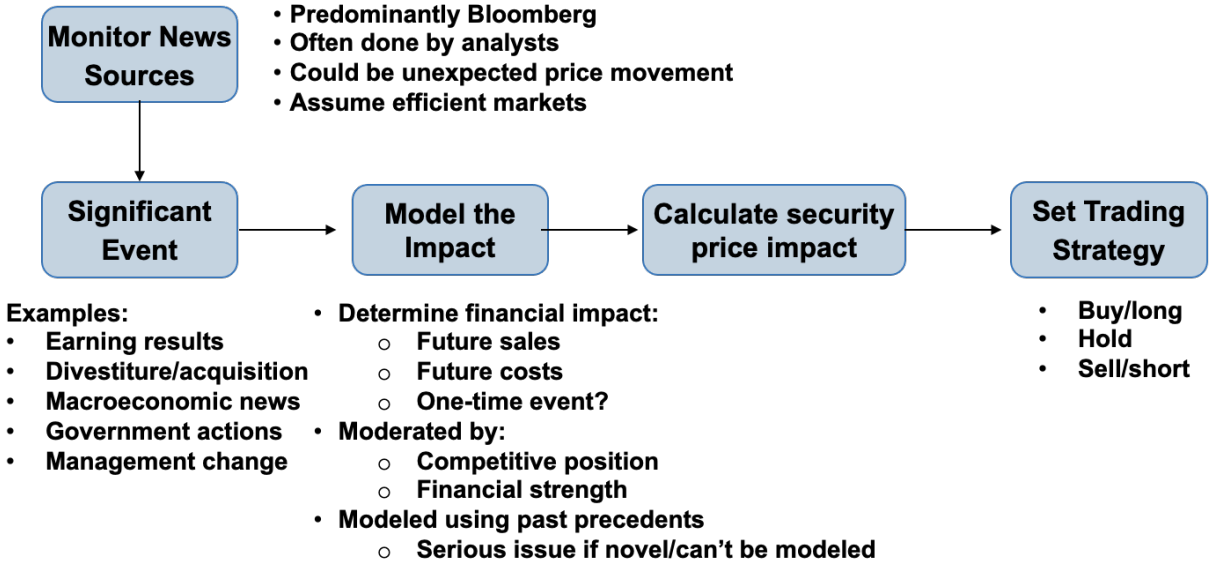
The interviews were semi-structured and lasted between 30 and 60 minutes. Initial questions, used to frame the subject and guide the interview, are shown in Table 10. The questions were emailed to participants prior to the interview. Some participants provided written responses to the questions prior to the interview.

The participant's role and interview dates are captured in Table 11. Interview notes were hand-written and then summarized in a memo. The memo captured key concepts and any follow-up questions. Follow-up questions were done via email or through additional interviews.

Data Analysis

Figure 15 illustrates the process by which institutional investors analyze and react to news events.

Figure 15: Process to identify, analyze, and react to news events



Those interviewed believe that the stock market is efficient, and that public news provides few arbitrage opportunities.

Their primary news source is Bloomberg, which is monitored for announcements and stock price changes. They will track mass media reports, such as those from the Wall Street Journal and CNBC, but mostly to anticipate questions from clients and senior management. Mass media reports did not influence trading strategy. None of the interviewees monitor social media or other non-traditional information sources.

Investors make a judgement call, using past experience, to determine whether the news is significant. Significant results lead to a recalculation of future earnings. For example, I interviewed two analysts who had covered the automotive industry. Recall announcements are significant. They would have used past recalls to model the future sales and cost impact of Ford's July 2021 Explorer recall (Hoffman, 2021), potentially leading to a change in share price guidance.

The worst negative events are those that are unprecedented and cannot be modeled. Two examples were cited by investors:

- First Energy bribery scandal: Five members of the Ohio House of Representatives were indicted for allegedly accepting over $60 million in bribes in return for their support of a nuclear plant bailout (Wamsley, 2020). Investors could not forecast First Energy's earnings because they were unsure of the scandal's effect on future rate increase requests. They liquidated their First Energy holdings, and the stock dropped 34% in two days.
- The 2018 California Camp wildfire[1]: A faulty Pacific Gas & Electric (PG&E) transmission line ignited what became the deadliest and most destructive wildfire in California history (Baldassari, 2018). California law holds a company liable for wildfire damages if their equipment is at fault, regardless of whether the company was negligent. Investors liquidated their shares because they could not model PG&E's future liabilities, and the stock dropped 51% within a week.

[1] The wildfire is named after its origin, Camp Creek Road.

Lawsuits, regulatory fines, and other one-time costs are generally dismissed as immaterial. Investors assume that a healthy firm will easily absorb the cost.

A company's competitive position determines whether on-going cost increases, such as raw material inflation, will impact future profitability. Investors expect that recurring cost increases lead to profit margin erosion in weaker firms, while stronger firms are able to pass the cost onto its customers.

Reactions To A Data Breach

Data breaches are viewed, in general, as inconsequential and immaterial. One portfolio manager confessed to having to look up examples to prepare for our interview. Another investor said that data breaches are the cost of doing business in the 21st century.

Investors do not believe that a data breach leads to a change in customer behavior. This position has been confirmed by extant research (Liang & Talang, 2020). A variety of reasons were given, such as breaches have become so ubiquitous that customers have become numb, and that consumers don't fully understand the ramifications of their personal information being stolen, Others referenced the power of brand loyalty and customer preferences,. One analyst who covered Target during its 2013 breach[2] noted that:

"*Customers pick Target because they like Target. They like the product offerings. They like the store location. They like seeing themselves as Target customers, whom they consider to be superior to Wal-Mart Customers. A data breach doesn't change that."*

She held her position, and was disappointed when Target's stock price didn't drop. She planned on increasing her holdings if it had.

[2] Target announced on December 18, 2013 that hackers had stolen 60 million credit cards.

The costs to remediate a breach are generally dismissed as a one-time charge against earnings and immaterial to future performance. Public pressure forces management to improve security, ensuring that the breach does not become a recurring event. Remediation costs, even for major breaches, are insignificant. Target 2013 data breach cost the company $162 million (Lunden, 2015), Target's 2013 net income was $1.97 billion. Equifax initially told investors that the cost of its breach would be $114 million[3]. Equifax's EBITA (earnings before interest, taxes, and amortization) for the quarter was $1.23 billion[4].

Investors also note that the majority of companies now have cybersecurity insurance (Table 8), which caps the cost of a data breach.

Investors did stress the importance of managing the breach. Management should have a pre-defined breach response plan as part of its crisis stakeholder confidence.

Investors did not believe that a data breach was necessarily a result of negligent management practices or poor cybersecurity capabilities. They felt that modern attacks have become too sophisticated to fully defend against, and that a breach could happen to anyone.

Data Breach Case Studies

Most interviewees referenced case studies to emphasize their points. A few are listed here.

<u>Target, disclosed on December 19, 2013.</u>

- The event: Hackers breached Target's internal network through a HVAC supplier. The hackers were able to steal over 60 million credit cards.
- Impact on share price: Closed at $62.52 on December 18th, $62.22 on December 19th. Closed at $62.79/share on December 27.

[3] Equifax's actual costs were close to $2 billion (Meltzer, 2020).
[4] The analyst also noted that Equifax's EBITA increased in the quarter after the breach.

- Analysis: The breach was considered novel at the time, and analysts were unsure how to model costs. But Target was considered an extremely strong company that could easily absorb any incremental charges. The consensus was that that future Target revenue and profitability would not change. The interviewees decided to hold their stock.

Equifax, disclosed on September 7, 2017.

- The event: Equifax failed to secure its web site, enabling hackers to gain access to the Equifax internal network. The hackers stole personally identifiable information of 143 million US citizens, including social security numbers, birthdates, and driver's license numbers.
- Impact on stock price: Equifax closed at $141.58 on September 6th, $141.45 on September 7th. The share price dropped to $94.40 by September 15th.
- Analysis: Investors were not concerned with Equifax's revenue. Equifax has two competitors and the industry has significant entry barriers. Customer switching costs are high because of the degree of systems integration, as evidenced by the industry's 3% customer churn rate.

  The stock dropped because of concerns with future liabilities and the management team. Investors could not estimate the cost of the breach because management's description of the breach kept changing. They were not confident management had a handle on the situation. Management never explained why they waited months after discovering the breach to announce it; there were allegations of insider trading[5]; and the website Equifax

[5] Jun Ying, Equifax's Chief Information Officer, was found guilty of insider trading for selling Equifax stock a week and a half before the breach disclosure. Two other executives, including the CFO, were investigated for equity trades made after the breach discovery but before breach disclosure.

provided for consumers was riddled with security errors. The Equifax CEO, CFO, and CIO eventually were forced to resign.

American Medical Collection Agency (AMCA), disclosed on June 3, 2019.

- The event: AMCA was hacked between August 2018 and March 2019, resulting in the theft of 26 million health records, including the patients of corporate clients such as Quest Diagnostics and LabCorp. AMCA is privately held, Quest and LabCorp are public companies.
- Impact: AMCA filed for bankruptcy. Quest stock went from $95.52/share on May 31st to $95.87 on June 3rd , to $99.62 on June 10th. LabCorp went from $161.99/share on May 31st to $162.88 on June 3rd, to $167.67 on June 10th.
- Analysis: The interviewees were not surprised that AMCA went bankrupt. One research analyst stated that "collection agencies are a dime a dozen, and easily replaced". The interviewees assumed that clients, such as Quest and LabCorp, would terminate their contracts to distance themselves from AMCA. They also believed that Quest and LabCorp would not be held responsible by their customers and regulators for an event originating at a third-party.

Colonial Pipeline, disclosed on May 7, 2021.

- The event: Colonial Pipeline is a private company which fell victim to a ransomware and data theft attack in May 2021. The attack halted the company's operations, leading to fuel shortages throughout the Eastern United States.
- The impact: Colonial's bonds held their value. Some interviewees were disappointed, they were hoping to buy "into the dip" if bond prices dropped.

- The analysis: Colonial Pipeline is viewed as a strong company in a non-competitive, heavily regulated industry. The ransomware demand ($4.4 million) was viewed as immaterial. Any future costs to improve cybersecurity defenses were assumed to be passed onto consumers, and the disruption in operation only delayed revenues. The interviewees did not feel the event had any impact on the company's credit quality or its ability to pay back its debt.

Implications For Companies

Investors view most data breaches as immaterial. The costs are insignificant, and will continue to decrease as cybersecurity insurance becomes more pervasive. Investors believe that data breaches do not change customer behavior or adversely impact future profitability.

Companies should be careful not to over-invest in cybersecurity. Companies should set a strategy of being "good enough" – implementing what is necessary to obtain the desired cybersecurity insurance policy, achieve regulatory compliance, and be consistent with generally accepted practices.

POLICY RECOMMENDATIONS

Introduction

A data breach is the unintentional dissemination of private information. Over 60% of Fortune 1000 companies have experienced a data breach in the past decade, and approximately 25% will suffer a data breach in the coming year ("Over 60% of the Fortune 1000", 2020). See Table 12 for the percentage of Fortune 1000 firms suffering a known breach between 2010 and 2018.

Cybersecurity consists of the defensive measures taken to prevent data breaches Data breach prevalence makes it natural to question whether firms are investing enough in cybersecurity. And if they are not, should the government intervene through regulations and by enforcing minimum standards?

Incentives To Invest In Cybersecurity

Firms motivated by economic returns will invest in cybersecurity if the expected marginal benefit exceeds the marginal cost. Benefits can be calculated as:

*(the reduction in the probability of a breach occurring * the cost of a data breach)*

The direct costs of a data breach include the cost to investigate the breach, the costs to implement corrective actions, legal fees, lost productivity due to business interruption, and the cost to notify customers. Firms suffering a data breach may incur regulatory fines and reputational damage.

Companies lack the information necessary to estimate data breach probability and costs (Mulligan, 2011). A comprehensive list of data breaches, including their cause and cost, does not exist. Firms do not willingly disclose this information because of the risk of negative publicity, lawsuits, and reputational damage (Moore, 2010). The lack of data means that

companies are at risk of over-investing if they are unduly influenced by practitioners who cite worst-case scenarios (Moore, 2010) or of underinvesting because they underestimate the odds and impact of a data breach. There is even debate on useful historical information would be if available. Today effective security control may be rendered obsolete by a new attack tomorrow. Understanding yesterday's attacks may not help prepare you for tomorrow's.

There is no generally accepted method to estimate the cost of a breach. Academic research has found that the cost of a breach varies based on firm size, industry, type of attack, the type of information lost, the number of records lost, and the quality of management's response (Huang, 2020). But the cost and impact of a breach may not consistent even after controlling for all of these variables. JP Morgan (2014) and Capital One (2019) both suffered data breaches of over 80 million customer records. Both are banks, neither lost personally identifiable, health, or financial data, both had high-quality management responses. JP Morgan's stock price increased after its breach announcement; Capital One's stock dropped 5.9%.

An alternative strategy is to use cybersecurity as a competitive differentiator. Surveys have found that consumers are concerned about cybersecurity (Morgan, 2020) and that they may be willing to pay a premium for it (Goldman, 2016; MacKinney, 2020). The issue with competing on superior cybersecurity, besides providing a tempting target to hackers who want to prove you wrong, is that consumers do not have a reliable way to measure relative cybersecurity quality. Past research, including a Noble-prize winning economics study, has shown that consumers will not pay a premium for quality that they cannot measure (Akerlof, 1970).

The economic rationale for investing in cybersecurity is, at best, nebulous. The lack of a credible quantitative justification is hindering efforts to improve cybersecurity. Over 70% of respondents to a UK survey on Cybersecurity Incentives and Regulations stated that the lack of

commercial incentives was a moderate to severe barrier to firms managing cyber-risks (Lam, 2021). A 2021 report from the Organization of Economic Co-Operation and Development (OECD) found that many cybersecurity challenges are economic in nature. These challenges include a lack of financial incentives (Lam, 2021).

Nebulous economic justification makes cybersecurity decisions susceptible to cognitive biases. Research has shown that humans exhibit a pervasive bias towards optimism (Sharot, 2011). They overestimate the likelihood of positive events and underestimate the likelihood of negative ones. Students consistently overestimate their job prospects and starting salaries; newlyweds underestimate their chances of getting divorced; and we consistently overestimate our ability (a survey found that over 80% of respondents believe that they are a better than average driver). Research has shown that a large majority of the population (approximately 80%) demonstrates optimism bias. A lack of optimism bias might be a sign of depression (Korn, et. al., 2013). People understand that bad things will happen, they just assume it will happen to someone else.

Optimism bias will lead to a company underestimating the cyber threats to their organization. They think that an attack is unlikely, and if it occurs, , the company overestimates their defense capabilities. Optimism bias may lead to minimizing the need for continuous improvements and investments in cybersecurity. Optimism bias may explain why a UK survey found that 43% of organizations experienced a data breach in the past year, yet only 67% of them spent spent money on cyber security measures in response (Department for Digital, Culture, Media and Sport, 2018).

Threat inflation, sometimes referred to as fear appeal arguments, is a political science concept use to galvanize action by creating concern. The presenter describes a fearful situation

that will happen unless you take the suggested action. Politicians routinely employ threat inflation to galvanize support for policy changes; sales reps can use threat inflation to encourage the purchase of their products and services.

There has been a consistent, steady, alarmist warnings of future cybersecurity threats. The argument is that cyberattacks are becoming increasingly sophisticated, pervasive, and catastrophic. Your company will eventually come under attack, and it will happen sooner rather than later. The company's on-going viability is at stake, because a data breach will ruin your company's reputation, lead to lost sales, and subject the company to punitive fines. But, taking this action (e.g., purchasing this cybersecurity product or service) will help stave off a cyber-attack induced disaster. Many emerging cybersecurity companies, such as Carbon Black, Dark Cubed, and DarkMatter, chose names that play on the perception that cyberspace is nether region in which the cybersecurity providers are the good guys fighting on behalf of unsuspecting and unprepared companies (Shires, 2020). Companies that fall victim to threat inflation will overinvest in cybersecurity.

Critics have charged that threat inflation has been used to push cybersecurity to the top of political agendas and public discourse (Gomez & Whyte, 2021; Brito & Watkins, 2011). The charge is that cybersecurity proponents, frustrated by a lack of progress, have deployed "cyber-doom scenarios". These involve hypothetical cyberattacks on a country's infrastructure, leading to physical harm, severe economic losses, and even social collapse. Critics are concerned that the use of cyber-doom scenarios encourages the adoption of counter-productive policies of control and centralization (Lawson, 2011) .

The lack of clear economic rationale, cognitive biases, and threat inflation make it hard for companies to determine an appropriate level of cybersecurity investment. It is also widely

acknowledged that no cybersecurity program can ever be 100% effective. Prudent firms should invest in products, such as cyber insurance, which minimize the financial impact of a data breach.

Cybersecurity Insurance

Industry overview

Cybersecurity insurance provides financial protection from the effects of a data breach. It typically reimburses the insured for the tangible costs of the breach, such as legal fees, lost productivity due to business interruption, ransomware payments, data recovery expenses, legal settlements, and regulatory fines. The insurance serves as a hedge, capping the insured's financial exposure..

Cybersecurity insurance is a growth industry, as firms seek financial protection from the unpredictable costs of a breach. The global market for cybersecurity is expected to increase from $7.8 billion in 2020 to $20.4 billion in 2025, a compounded annual growth rate of 21.2% (Greenwald, 2020).

Risks to the carriers

The insurance carriers face adverse selection risk. Like life insurance, the least desirable customers need the product the most; the best customers need it the least. And like life insurance, insurers manage adverse selection risk through the underwriting process. Cyber insurers will perform a security assessment prior to issuing a new policy. The assessment is primarily done through a carrier-specific questionnaire, supplemented as necessary by interviews, client-led presentations and site visits. The goal is for the carrier to get enough

information from the applicant to model the likelihood of a future data breach. A typical questionnaire asks about the implementation of specific security controls, the amount, storage, and handling of sensitive data, the number and locations of employees, and the company's cybersecurity processes. Like life insurance, a misrepresentation during underwriting can void the policy and any subsequent claims.

A moral hazard occurs when a party does not suffer the full consequences of a risk. The party receiving protection may act differently than they would if they were not protected. Employees take less care of their office laptops than their personal technology. Critics charge that the government bail outs during the great recession of 2007-2009 encourage the risky investments, accounting blunders, and inefficient operations which lead to financial crises. Companies with cyber insurance may forego future cybersecurity investments.

Ransomware has brought cybersecurity insurance moral hazard risk to the forefront: The industry is accused of inadvertently encouraging the growth of ransomware attacks. It is cheaper and less disruptive for the victim with insurance to pay the ransom and file a claim than to incur the costs of rebuilding the IT infrastructure, suffering through a business interruption, and risking reputational damage and negative publicity. Criminals know this and try to target firms with cyber insurance. They have attacked insurers in order to get their client lists. They try to determine the victim's coverage amount prior to setting the ransom (Bajak, 2021). Criminal entrepreneurs have introduced Ransomware as a Service (RaaS) offerings to make it easier to execute an attack (White, 2021). Table 13 displays example RaaS advertisements. The result is the number of ransomware attacks on organizations doubled during the first 6 months of 2021 (Cogntyte Research Group, 2021); the number of attacks on the banking industry increased by 1,381% (Henriquez, 2021); and insurers have seen a 400% increase in annual ransomware claims

(Bajak, 2021). Researchers noted that "Cyber insurers are unintentionally facilitating the behavior of cyber criminals by contributing to the growth of targeted ransomware attacks" (MacColl, et. al, 2021).

Insurers have responded by increasing premiums by over 100%. Leading carriers have started excluding ransom payment coverage from new policies (Kass, 2021). The criminals are fighting back: Axa, who is the US market leader, announced on May 9th, 2021 that it would no longer write policies that reimburse ransomware payments. Axa was a victim of a ransomware attack within a week (Avast Security News Team, 2021).

Opportunity to use cyber insurance to improve overall cybersecurity

Cyber insurers have the potential to become the de facto regulator. Insurers can set and enforce minimum cybersecurity standards. Companies who want the financial protection have a strong incentive to implement the security controls and processes prescribed by the insurers. Influential cybersecurity author Brian Schneir predicted that cyber insurance carriers would eventually subsume the computer security industry (Schneir, 2001). The claims and controls data can be aggregated and shared, helping all parties understand the risk, frequency and costs of a data breach. The potential benefits have led to calls for making cyber insurance mandatory (Lemnitzer, 2021).

This potential is not being realized. Competition, and the push to grab market share in a nascent, rapidly growing industry limits the carriers willingness to set minimum cybersecurity standards. Competition also limits data pooling and sharing. Claims data is seen as the source of competitive advantage: It is the basis for a company's risk models, product design, and pricing. Sharing this information eliminates the advantage of obtaining the data, and makes it easier for

new insurers to enter the market. Data privacy is yet another issue: Customers don't want their security controls and claims history made widely available. The regulators I interviewed did not see insurance carriers ever willingly sharing their data. The unrealized potential of cybersecurity insurance has led some researchers to call for government intervention (MacColl et al,, 2021; Lemnitzer, 2021).

It is important to note that while cybersecurity insurance has the potential to facilitate cybersecurity improvements, it is not its primary purpose. Its purpose is to help companies manage residual cyber risk through financial protection. Carriers will always act in their own interests and take actions which maximize their profits. Regulatory action may be a better way to force cybersecurity improvements.

Regulatory Options

A market failure occurs when economic incentives lead to an inefficient allocation of resources. A neighborhood receives benefits from a new park or library, the economy as a whole benefits from an improved transportation infrastructure. But it is not in the best interests of any individual party to pay for something that benefits the whole. The free market will underproduce these types of goods and services.

Externalities are closely associated with market failures, and occur when an economic decision made by one party impacts an independent third-party. Externalities can be either positive or negative. A positive externality occurs when the project benefits someone other than the producer, such as a new park or better highways. A negative externality occurs when a decision results in costs to a third party. A firm polluting a lake with runoff chemicals adversely impacts the local community who depend on the lake for drinking water and recreation. Market

failures and externalities are used to justify government intervention through projects, actions, and regulations.

Some have argued that cybersecurity suffers from negative externalities. The internet is a shared resource, so cybersecurity decisions at one firm can impact everyone else. Undetected malware at one company can become part of a botnet used to attack other firms. A breach resulting in the disruption of a critical infrastructure industry (such as the delivery of electricity) could result in massive losses to the economy as a whole. In 2013, hackers obtained access to Target's network by attacking one of its HVAC suppliers. The hackers stole 40 million credit cards, and Target paid $18.5 million in settlements (Abrams, 2017). Vulnerabilities in shared software, such as the recent SolarWinds and log4j issues, have put thousands of government agencies and private firms at risk.

Governments may look at data breach frequency, the lack of a clear return on investment, the costs data breaches have on other firms, infrastructure, citizens, and the economy as a whole, and decide that intervention is needed. They may decide that businesses are not investing enough in cybersecurity and that new regulations are needed.

Ex-Ante (before the event) Regulations

The challenge is implementing effective, relevant regulations that are effective and do not create new problems. Defenses evolve and improve as new threats emerge. Prescriptive standards will need to be revised at the pace of technical change or risk becoming ineffective and irrelevant. This may not be realistic, since the process for designing and agreeing to standards can take anywhere from a few months to a few years (Srinivas, et. al., 2019). And standards may not prevent data breaches. The payment card industry created the Payment Card Industry Data

Security Standard (PCI-DSS) to establish standards for the storage, processing, and transmission of cardholder data. Target was certified as PCI-DSS compliant a few weeks prior to its December 2013 data breach of 41 million payment cards (Moldes, 2018). An alternative is to create general regulatory guidelines that are directional in nature. But they are open to interpretation and may lack the specificity necessary to drive cybersecurity improvements.

Legal scholars have found that regulatory standards are ineffective when the appropriate standard is uncertain (Moore, 2010). The link between cybersecurity standards compliance and a reduction in vulnerabilities is unproven (Mulligan, 2011), and a study found that a majority of firms believe that compliance with regulatory standards has a negligible impact on overall security (Dynes, et. al, 2013).

The myriad of issues regarding establishing minimum cybersecurity standards has some researchers calling for outcomes-based regulations. Outcome-based regulations focus on desired results rather than detailed rules. It started gaining political momentum as a better way to regulate capital markets in both the US and Europe prior to the 2007-2008 financial crisis (Black, 2008). The theory is that the organizations and their management are best suited to determine the processes, technologies, and actions necessary to efficiently and effectively meet an objective set by regulators. This, in theory, gives regulated firms the flexibility to rapidly adopt new practices and technologies in complex, rapidly changing environments.

The issue, for both regulators and the regulated, is that outcome-based approaches remove certainty and predictability. Firms cannot be sure that their actions are sufficient for compliance, as it may vary by regulator. The benefit of outcome-based regulations is that organizations can quickly adapt new cybersecurity technologies, but in practice, they may have to educate and convince their regulatory body of their validity. Firms may decide it is easier to stay with

incumbent solutions until the new approach is generally understood and accepted, which could make cybersecurity worse.

The challenges of establishing and updating effective standards may explain why there has been little new US cybersecurity regulation since the July 2019 passage of the New York SHIELD (Stock Hacks and Improve Electronic Data Security) Act.

Ex-Post (after the event) Regulations and Liabilities

Standards, both prescriptive and outcomes-based, are examples of ex-ante (before the event) regulation. The goal is to prevent data breaches by requiring safeguards which prevent data breaches from occurring. An alternative and often complementary approach is ex-post (after the event) regulation. Ex-post regulation levies fines and financial penalties against the firm responsible for a data breach. The theory is that the threat of future monetary damages will encourage firms to invest in cybersecurity.

US government agencies have used their authority to start levying cybersecurity penalties. The Federal Trade Commission (FTC) can take action against companies who use deceptive advertising and dishonest sales tactics. The FTC has used this authority to issue fines against companies who have experienced a data breach. The FTC's position is that companies were dishonest when they collected and committed to protecting a customer's personal information. Example FTC cases include Facebook, BJ Wholesales Club, and Kohl's Department Stores. The US Security and Exchange Commission (SEC) requires that publicly-traded companies disclose all material events. It issued guidance in 2011, with supplemental clarifications in 2018, to remind firms that cybersecurity lapses, data breaches, and vulnerabilities can be material events. It issued its first fine and a cease and desist order against First American Financial Corporation

on June 15, 2021. First American had not, per company policy, closed a vulnerability which led to the exposure of over 800 million customer images. The SEC charged First American with failing to maintain disclosure controls and procedures to ensure that information about the vulnerability was made available to investors (SEC, 2021).

The issue with ex post regulations is that they may not spur cybersecurity investments. Companies do not know if or when they will suffer a data breach. Nor can they predict the breach's severity and the regulatory reaction. Companies may become indifferent to the risk of future financial penalties since they cannot be predicted. And most people, including corporate decision-makers, demonstrate present bias. Present bias is the tendency to settle for a smaller immediate reward rather than wait for a larger future payoff (O'Donoghue & Rabin, 1999). The costs of investing in cybersecurity are tangible and have an immediate impact on the bottom line. The benefits, such as a reduction in potential regulatory liabilities, are nebulous, may be less than the required investment amount, and if realized, occur sometime in the future.

As an example, the PCI-DSS cybersecurity standard was established by the major credit card brands (the founders were American Express, Discover, MasterCard, Visa, and JCB International) to prevent credit card theft. Non-PCI compliant firms that suffer a breach are subject to fines from the PCI governing council. A 2020 Verizon study found that only 27.9% of organizations are fully PCI compliant, a percentage that has dropped steadily since 2016 (Verizon, 2020).

There is also the question on whether a data breach that led to find could have reasonably be prevented. Two regulators I interviewed referenced Anthem. Anthem was the victim of a sophisticated Chinese-sponsored attack in 2015, resulting in the theft of 79 million customer health information records (Krebs, 2015; McGee, 2021). Anthem was fined $16 million by the

Department of Health and Human Services. Anthem had passed all of its regulatory examinations prior to the breach, and was generally viewed as a company with an outstanding cybersecurity program.

Companies could analyze the Anthem breach and the subsequent fine, and decide that it is better to invest in cyber insurance and transfer any future regulatory liability to the insurer rather than make incremental investments in cybersecurity.

Disclosure laws

California passed the first data breach disclosure law in 2002. The rest of the United States, and many countries around the world, quickly followed suit. Today, all 50 states and an additional 90 countries have some form of a notification law. The law requires companies to notify individuals affected by a data breach involving their personally identifiable information (PII). The laws also typically require the company to offer some type of remediation service to affected individuals, such as free credit monitoring.

The goal of data breach notification laws is two-fold. The first is a belief that the individuals have the right to know. This enables them to take actions to protect themselves against identity theft and financial fraud. The second is that notifications will highlight a firm's poor security controls. This creates incentives for firms to improve their cybersecurity to avoid incurring the notification and remediation costs and eliminate the reputational risk from the resulting negative publicity. The UK Science and Technology Committee stated that the "data breach notification law would be among the most important advances that the United Kingdom could make in promoting personal internet security (House of Lords, Science and Technology Committee, 2007).

The SEC has based its regulations on mandatory disclosures, the theory being that disclosures promote market efficiency and ensures a well-informed investing public. The SEC has increased its emphasis on cybersecurity disclosures (Rabinowitz, 2021). 2011 SEC guidance reminded companies that they must disclose all material events, and that material events may include cybersecurity risks and incidents. The expanded guidance issued in February 2018 stated that cybersecurity risk is a threat to investors, capital markets, and the country as a whole (U.S. Security and Exchange Commission, 2018). Companies have an obligation to disclose cybersecurity risks and incidents in a timely manner, including material risks that have not yet been the target of an attack or have led to a successful exploit (Cain, et. al., 2021). Public statements and official guidance have emphasized that employees with knowledge of the company's security vulnerabilities have an obligation to share that knowledge with those responsible for making SEC disclosures.

The argument in favor of mandatory disclosures can be summarized by the phrase "sunlight is the best disinfectant". The phrase comes from U.S. Supreme Court Justice Louise Brandeis, who argued that making the actions of government officials more visible helps eliminate government corruption. Likewise, forcing companies to disclose their data breaches and their cyber risks serves as a powerful incentive for companies to improve their cybersecurity.

Critics counter that disclosure laws create unnecessary costs for firms and consumers. Markets regulate themselves: If notifications are valued, investors and consumers already favor firms that voluntarily disclose their risks and data breaches. They note that only a small percentage of data breach victims, roughly 2%, become victims of fraud. The majority of this fraud is committed on existing credit accounts where the liability is born by banks, credit card issuers, and merchants, not the individual (Lenard & Rubin, 2006). A study found that data

breach disclosure laws had a marginal effect on identity theft (Romanosky, et. al., 2011). Consumers may become indifferent to the notifications if they are inundated with them. Writers have referred to this as data breach fatigue (Rokkex, 2019). There is evidence that consumers no longer take action after a breach, such as changing compromised passwords (Mello Jr., 2021).

Research has found that the SEC disclosure guidance may be counter-productive and limiting the value of cybersecurity disclosures. A study examining disclosures prior to the SEC's 2011 guidance found a positive link between a cybersecurity risk disclosure and the occurrent of a future data breach (Wang, et. al., 2013). A post-guidance study found that disclosures no longer predicted a future breach. The authors' conclusion was that all firms were issuing cyber risk disclosures, regardless of materiality, in order to mitigate future litigation and regulatory costs (Li, et. al, 2018).

Policy Recommendations

What not to do: Regulations that establish standards, increase fines

The argument for increased cybersecurity regulation is straightforward and makes intuitive sense. Companies with poor cybersecurity can be compromised and used as bots to attack other firms, putting everyone at risk. Organizations which manage critical infrastructure services are at risk of cyberattacks from terrorists and state-sponsored hackers. A successful cyberattack against the power grid, such as what happened to the Ukraine in December 2015, would be devastating to citizens and the economy. Organizations do not bear the full costs of a data breach. This distorts economic incentives, leading to the under-production of cybersecurity. Cybersecurity is a market failure. The government needs to intervene.

This argument is overstated. Most contemporary attacks, including the attack on the Ukraine power grid, are launched directly against the target. The SEC and sector-specific government agencies already have cybersecurity oversight responsibility (Fisher, 2014) and the agencies should already be working with the private sector to ensure that organizations have adequate defenses. Successful, crippling cyberattacks against critical infrastructure are low-probability, high-impact events. Firms and regulators should focus on early warnings (security incident detection), resilience, and recovery. The power grid is designed to withstand and recover from weather events and natural disasters. The same principles can be applied to cybersecurity attacks.

The calls for increased regulations and standards are based on an assertion that private companies underinvest in cybersecurity. That may be an unfair, or at least premature, assertion. The appropriate level of cybersecurity investment depends on the likelihood and cost of a data breach. There is not a generally accepted methodology to make the appropriate calculations. There has not been an empirical study on the current level of investment compared to an ideal, with the ideal considering the costs to society as a whole. I believe that because of the absence of data and the use of scare-tactics and threat inflation, organizations are just as likely to be over-investing as under-investing in cybersecurity.

New regulations and standards are unnecessary, impractical, and could be counter-productive. Defenses and threats evolve far faster than regulatory change. The standards will be outdated as soon as they are issued. Cybersecurity is a complex ecosystem; the effects of regulation on complex systems are unpredictable (Clark-Ginsberg & Slayton,2018). Government-imposed standards could make the problem worse, replacing a perceived market failure with a government-failure.

What can be done: Regulations to increase Information Sharing

The cybersecurity industry suffers from a lack of information. It is almost impossible for an individual firm to estimate the likelihood and the cost of a data breach, making cybersecurity investment decisions difficult. Firms are at risk of under-investing in cybersecurity (if they underestimate the risk because of ignorance or optimism bias) or over-investing (if, for example, the firm falls for threat inflation). Empirical studies are needed to determine if the private sector investing at an appropriate level, or, if under-investing, to establish the need for further regulatory intervention.

The lack of information hinders responses to emergent systematic risks. Hackers, believed to be directed by the Russian Intelligence service, inserted malicious code into a routine update of SolarWinds' Orion software. Orion is a popular IT infrastructure management application used by over 33,000 customers (Temple-Rason, 2021). The Orion customer base includes banks, hospitals, government agencies, and 25% of North America's power utilities (Watson, 2021). The Department of Homeland Security reported that over 100 companies suffered a data breach because of the SolarWinds vulnerability, including technology leaders Cisco, Microsoft, and FireEye (Bing, et. al, 2021). The SEC, in order to get better visibility into the extent of the attack, has asked companies to voluntarily report any cyber incidents caused by an exploit of the SolarWinds vulnerability (Kovar, 2021). The SolarWinds cyberattacks highlight the systematic risk created by the use of common software applications. The SEC probe highlights the lack of information available to firms, cybersecurity professionals and policy makers as they organize defenses and assess damages.

Cyber insurance carriers are the natural aggregation points for collecting data breach data but they will not do so voluntarily. As one insurance executive stated "Insurance is data" (MacCool, et. al, 2021). The insurer's data is their competitive advantage, sharing the information broadly levels the playing field and encourages new entrants. Sharing data will turn cybersecurity insurance into a commodity with eroded profit margins. The rational carrier strategy is to initially underwrite as many policies as possible in order to accumulate data, then use the data to make superior risk models. The carrier is now positioned to make superior underwriting decisions, leaving the unprofitable customers to the competition.

The government needs to intervene to fill the information gap. If there is systematic under-investment in cybersecurity it is driven by inaccurate cost and probability estimates which are leading to understated return on investment (ROI) calculations. Government should provide the information necessary to make accurate decisions, and then trust the market to act rationally.

Regulators should start by expanding existing data breach disclosure laws. All 50 states currently have a disclosure law, whose primary motivation is to notify affected individuals so that they can take protective actions (Romanosky, et. al. 2011). Legislative details vary, but in general, the existing laws only apply to the loss of personal information. Disclosures should be expanded to include all types of cyberattacks, such as ransomware, intellectual property theft, and denials of service. The government will have to take responsibility for redacting all sensitive information, the stewardship of the data, and indemnify companies who share security information from lawsuits and privacy viiloations. The redacted information can then be made available to companies and researchers to better understand the costs, probability, and causes of data breaches.

Two recent proposals are steps in the right direction. Ransomware is making headlines, but nobody really knows how pervasive it is. The Ransom Disclosure bill, sponsored by Senator Elizabeth Warren and Representative Deborah Ross, will increase visibility by requiring companies to disclose ransomware payments to the federal government (Wider, 2021). An additional bill, the bipartisan Cyber Incident Notification Act, was drafted in response to the SolarWinds and Colonial Pipeline attacks (Feiner, 2021). Testimony to the Senate Select Committee on Intelligence stated that the government only became aware of the SolarWinds hack because of a FireEye report to its customers. The bill requires federal agencies, federal contractors, and critical infrastructure companies to notify the Department of Homeland Security (DHS) of any breach of their systems. The DHS is required to anonymize personally identifiable information, and companies who share information receive limited legal immunity (for example, shareholders who file a lawsuit cannot get access to the disclosed information). The goal is to increase transparency and to coordinate responses to cybersecurity events.

Finally, the government should add value to the data by entering into partnerships with managed security service providers, external threat intelligence suppliers, and cloud service industry in order to contextual information to the data. This approach will increase visibility and help prepare defenses for vulnerabilities which are actively being exploited. It would help the industry discover sources of systematic risk. Cyber insurers could aggregate and interpret the information and then advise their clients on how to take remedial actions.

Finally, the government should add value to the data by entering into partnerships with managed security service providers, external threat intelligence suppliers, and cloud service industry in order to contextual information to the data. This approach will increase visibility and help prepare defenses for vulnerabilities which are actively being exploited. It would help the

industry discover sources of systematic risk. Cyber insurers could aggregate and interpret the information and then advise their clients on how to take remedial actions.

Future Research

One motivation for disclosure laws is that firms will improve their cybersecurity defenses in order to avoid the negative publicity and outraged customers that will come from a data breach. The UK Science and Technology Committee went so far as to state that "data breach notification law would be among the most important advances that the United Kingdom could make in promoting personal internet security (House of Lords, Science and Technology Committee, 2007). Discussions on the economic consequences of a data breach include the threat of reputational risk, which is the loss of market share after the data breach due to the damage done to the firm's reputation.

However institutional investors believe, and at least one academic study confirms (Liang & Tulang, 2020), that customer behavior does not change as a result of the breach. This implies that reputation risk due to cybersecurity events is a myth. Articles have stated that, rather being outraged, consumers are numb and indifferent to date breaches (e.g., Kvocko & Pant, 2015; Mele, 2018). It has been suggested that customer indifference is due to some combination of not understanding the impact of a breach and the consequences of identity theft; being overwhelmed by the sheer volume of data breach notices; switching costs; and a lack of confidence that a competitor's cybersecurity will be any better.

Future research is needed to understand data breaches from a consumers perspective. The research agenda should include their perception of the risk, what they say would lead to a change in their buying patterns v. what they actually do, and their perception of data breach prevalence.

This research would be extremely helpful to practitioners setting a cybersecurity security as well as to policy makers considering enhanced disclosure laws or who are developing consumer education programs.

Tables

Table 1 – Extant research: Effects of a data breach

Authors	Analysis	Conclusion
Campbell, Gordon, Loeb, and Zhou (2003).	Effect of a security breach on publicly traded US firms share price.	Depends on the nature of the breach. Negative impact if the breach involves unauthorized access to information. No impact otherwise.
Morse, Rival, and Winegender (2011).	Impact of a data breach on stock price.	Firms suffering a breach will experience abnormal negative returns, moderated by whether the breach could have been prevented with reasonable precautions.
Gordon, Loeb, and Sohail (2010).	Market reaction to voluntary cybersecurity disclosures by looking at US SEC filings from 2000-04.	Positive reaction to proactive investments. Positive reaction to vulnerability disclosures. No reaction to actual breaches.
Song, Cavusoglu, Lee, and Ma (2020).	Determine if voluntary IT risk disclosures increase a firm's risk of a stock price crash.	Firms that disclose IT risks in their disclosures have a heightened, statistically significant risk of a stock price crash.
Holgan, Olsson, and Angelina (2020)	Market value impact of a data breach.	Abnormal negative returns in the short-term, but smaller than previous studies.
Kamiya, Kang, Kim, Milidonis, and Stulz (2020).	Quantify the reputational loss impact of a data breaches.	Defined reputational loss as the difference between the change in market value and breach mitigation costs for breaches which occurred between 2005 and 2017. Study found no reputational loss if the breach did not involve personal financial information, large cost otherwise.
Kannan, Rees, and Sridhar (2007).	Determine the long-term financial impact of a data breach announcement.	Breached firms do not suffer significant negative returns over the long run.
Bharadwaj, Keil, and Mähring (2009).	Impact of IT failures, which impact operations are failed new projects, on the market value of firms.	Paper found, by looking at 213 IT failures between 1990 and April 2000, an average decline in market value of 2%.
Haislip,Kolev, Pinsker, and Steffen (2019).	Analyze the market effect of a data breach on other firms in the industry.	No significant statistical impact on other firms in the industry.
Yayla and Hu (2011).	Impact of market value on firms due to a cybersecurity issue.	Paper looked at 130 cybersecurity events from 1994 to 2006. Found that denial of service attacks, which disrupt website operations, had the most material impact. Paper found the impact was less severe for more recent events.
Telang and Wattal (2007).	Impact of vulnerability announcements on the	Average market cap loss of 0.63% on the day of the vulnerability announcement. No statistically significant change either before the announcement or after the day of

	value of software companies.	the announcement. The loss is greater if a patch fixing the vulnerability is not also announced.
Richardson, Watson, and Smith (2019).	Impact on stock price of breached firms.	Nominal impact immediately after a breach (-0.3%). No impact after a short time window, except for the most severe data breaches.
Schatz, and Bashroush (2016).	Examined the influence of one or more data breaches on the stock market value of a firm.	Did not see a statistically significant decrease in share price after a breach announcement (after removing an outlier). Statistically significant with the outlier. No statistically significant impact after a second breach. Statistically significant if all events are analyzed (decrease of 1.27%), leading the authors to assume a "weak" confirmation that firms which suffer a data breach suffer a decrease in market value.
Goldstein, Chernobai, and Benaroch (2011).	Impact on market value of an IT loss event.	Data breaches do not have impact market value. Other loss events (e.g. an extended outage) have a statistically significant negative impact.
Gordon, Loeb, and Zhou (2011)	Impact of a breach on stock market returns.	Impact on firms is significant, but breaches that effect availability are more significant than those that impact confidentiality or data integrity. Impact is decreasing over time. Authors speculate it is because investors are lowering their assessments of the impact of a data breach.
Cavusoglu, Mishra, and Raghunathan (2004).	Impact of a breach on a firm's market value. And, through information transfer, the impact on security developers.	Breached firms lose, on average, 2.1% of their market value two days after the announcement. Internet firms lost more market value then traditional firms. Security developers, on average, realized a 1.36% increase two days after the announcement.
Liang and Talang (2020)	Impact of the 2014 Home Depot data breach on consumer purchasing behavior.	No effect. Consumers purchased the same amount, with the same payment card type, after the breach as they did before the breach.
Cheng, and Waltan (2019).	Studied how non-professional investors react to data breach disclosures.	Overall negative impact. Less negative if the company makes the disclosure quickly after the breach occurs. More negative if an external party announces the breach after a significant time lag between the breach and the announcement.
Juma'h, and Alnsour (2020).	Analyze the effect of data breaches on a firm's intermediate (quarterly) performance.	Financial performance, such as ROA and ROE, declined the quarter of a data breach. The firm's market valuation did not change.

Table 2 – Extant research: Market valuation

Authors	Breach period, # breaches	Data Source	Method	Data breach impact on market valuation
Ali, Lai, and Shad (2021)	2011-2019	Privacy rights clearinghouse.	Buy and hold abnormal returns by comparing breached firm to a firm in same industry and of similar size.	No abnormal returns compared to the matched firm six months prior to the breach. Significant negative abnormal returns in the year after the breach.
Campbell, Gordon, Loeb, and Zhou (2003).	1995-2000, 43	5 newspapers	Event study; Capital asset model	Significant; negative
Cavusoglu, Mishra, and Raghunathan (2004).	1996-2001; 66	Lexis/Nexis; CNET; ZDNET	Event study; Capital asset model	Significant; negative
Kannan, Rees, and Sridhar (2007).	1997-2003; 72	Wall Street Journal; NY Times, CNET; ZDNET	Event study; Capital asset model	No significant relationship
Morse, Rival, and Winegender (2011).	2000-2010; 306	5 newspapers	Event study; Capital asset model	Significant; negative
Gordon, Loeb, and Zhou (2011).	1995-2007; 121	5 newspapers	Event study; Fama French 3 factor model	No significant relationship
Yayla and Hu (2011).	1994-2006; 123	Internet search and Lexis/Nexis	Event study; Capital asset model	No significant relationship
Schatz, and Bashroush (2016).	2005-2015; 50	Privacy Rights Clearinghouse	Event study; Market model methodology	No significant relationship
Richardson, Watson, and Smith (2019).	2005-2017; 827	Privacy Rights Clearinghouse	Event study; Fama French 4 factor model	No significant relationship
Hogal, Olsson and Angelina (2020)	1990-2019; 3,931	Database from Advisen LTD	Event study; Capital asset model	Significant; negative

Table 3 – Number of breaches and millions of records lost per year
Source: *Identity Theft Resource Center*

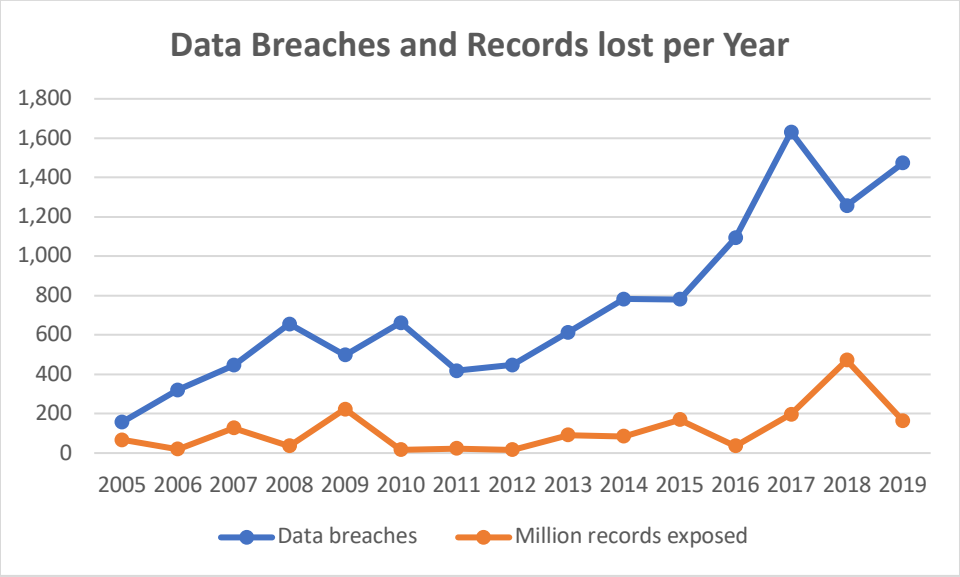


Table 4: Worldwide Cybersecurity Spending by Year
Source: *Gartner*

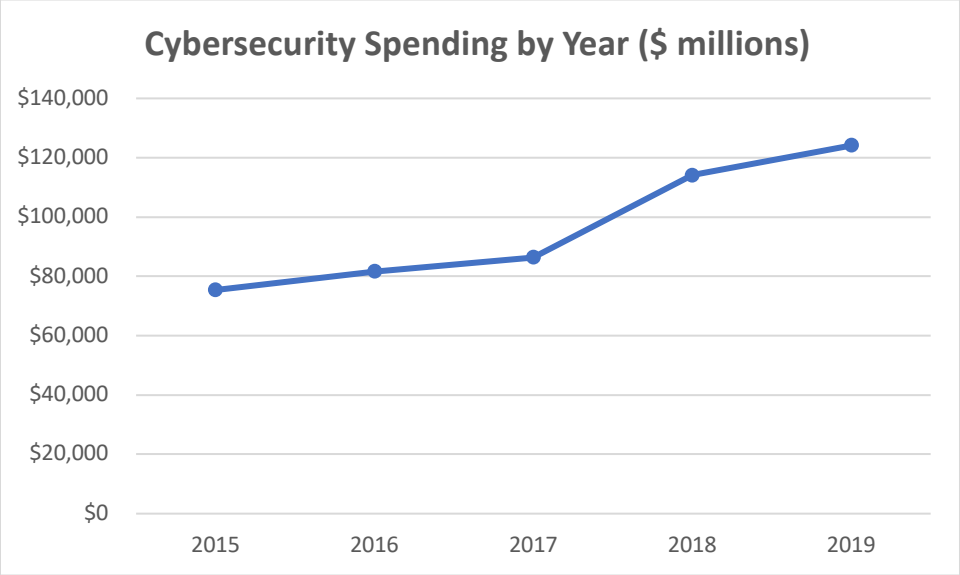


Table 5: Stock price movement before and after a data breach. Selected Stocks.
Source: *Yahoo*

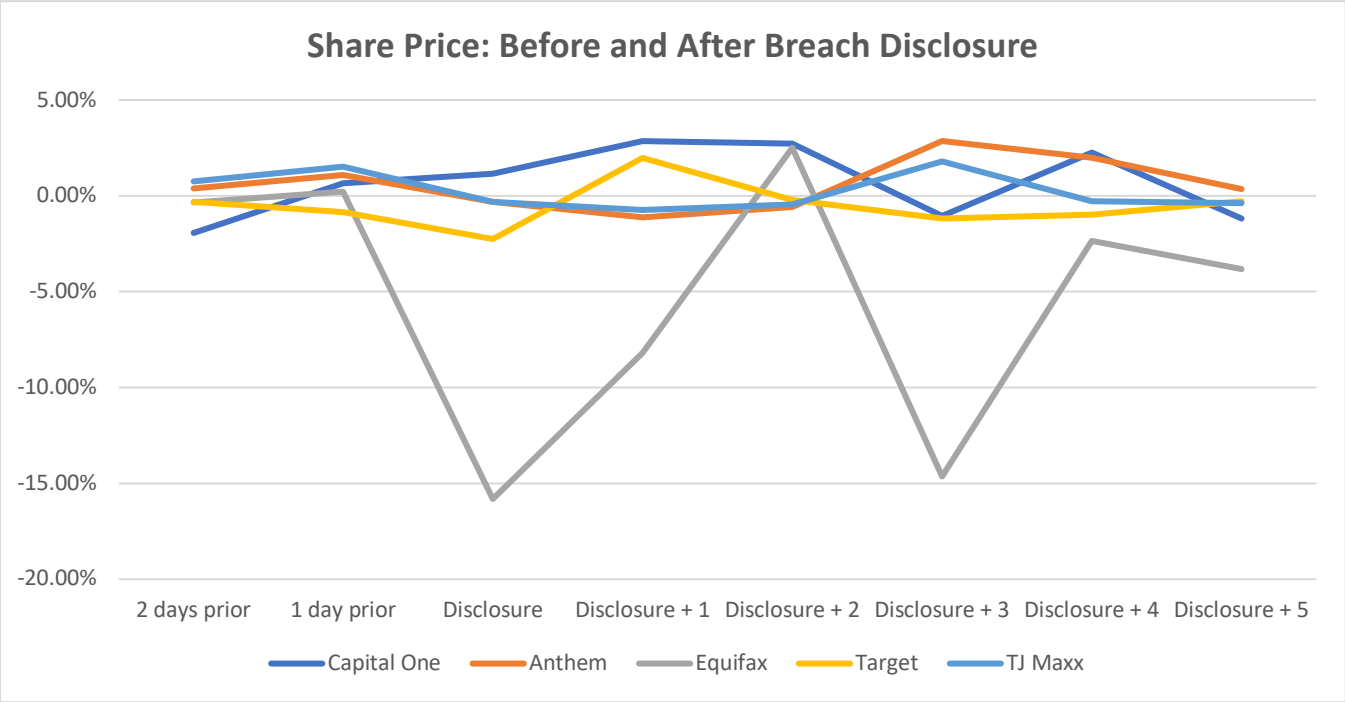


Table 6: Average Costs of a Data Breach by Year (Global)
Source: *IBM Security/Ponemon*

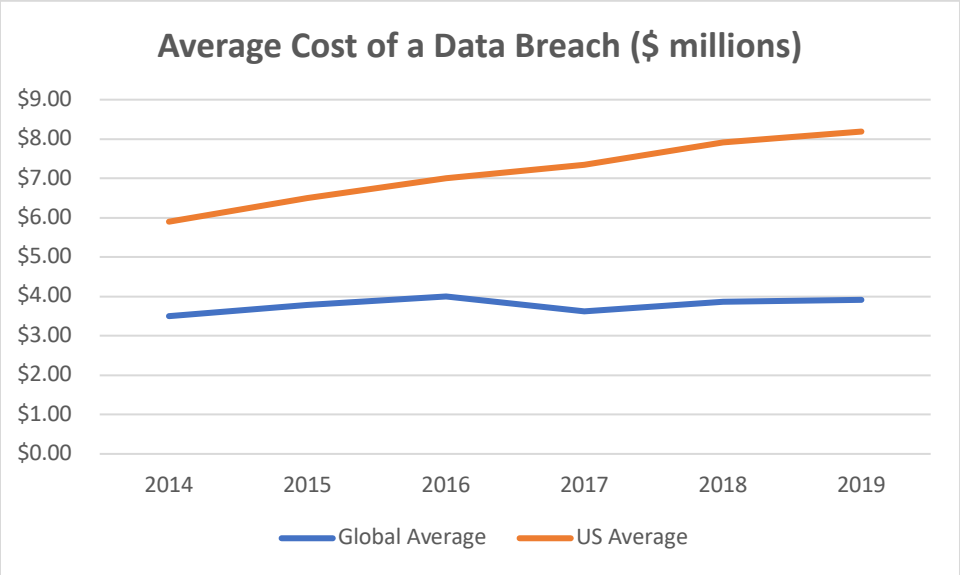


Table 7: US Data Breach Costs: Per record, by industry
Source: *IBM Security/Ponemon: 2019 Cost of a Data Breach Study*

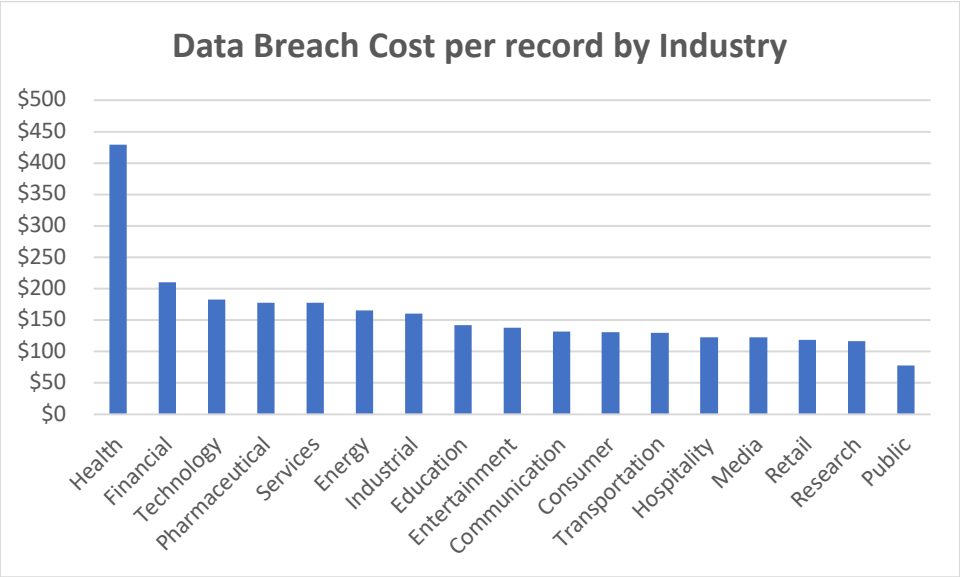


Table 8: Cybersecurity Insurance Adoption
Source: *Statista Research Department, November 5, 2020*

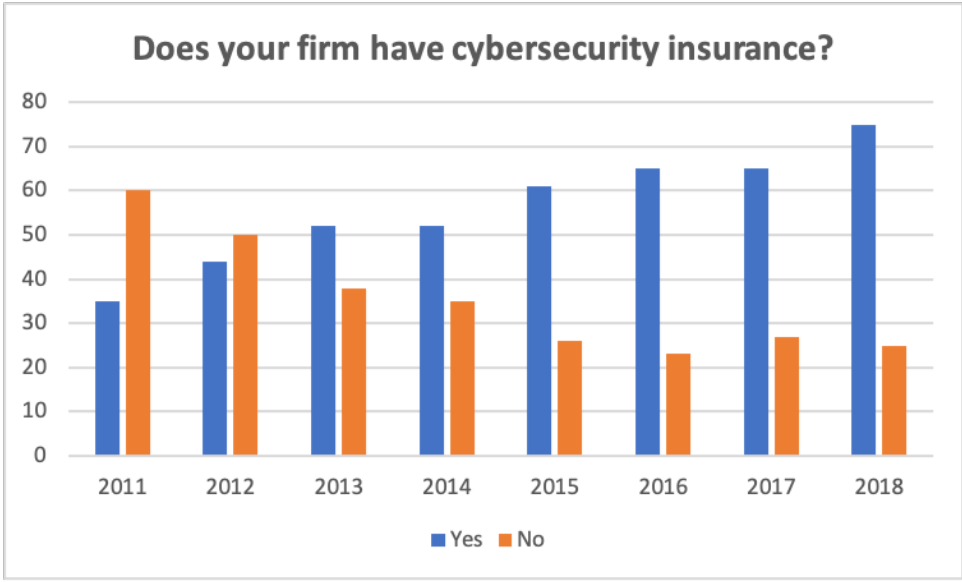


Table 9: Investor reaction to new information

Authors	Analysis	Conclusion
Barbens, Shleifer and Vishny (1997).	Presents a model that explains underreaction of stock prices to earnings announcements and over- and under-reactions to other events.	Created a model based on the representativeness heuristic (tendency to ignore chance and probability) and conservatism (individuals are slow to change their impressions). Proposed model assumes investors believes investors underreact to surprises/news/events. Proposed model assumes investors overreact to a string of consistent news. Authors believe this explains the anomalies, which challenge the efficient market hypothesis.
Barber and Odean (2005).	Test the hypothesis that investors are net purchasers of attention-grabbing stocks, such as those in the news	Confirmed that individual investors are more likely to purchase attention-grabbing stocks, and that these stocks will under-perform relative to stocks sold by individuals.
Boudoukh, Feldman, Kogan and Richmardson (2012)	Past research has found little relation between stock prices and news, violating a tenet of financial economics. The paper re-tested the relationship between news and stock prices using contemporary artificial intelligence technology.	Found evidence of a strong relationship between news and stock prices, especially when the tone of the news is taken into account.
Cutler, Poterba and Summers (1989).	Paper studied the amount of stock price variance which can be explained by various types of news.	Found that it was difficult to explain market movement based on publicly available news. This conclusion castd doubt on whether stock price movements can be explained by news and discounted cash flows.
Daniel, Hirshleifer, and Subrahmanyam (1998)	Use Attribution Theory from psychology to assume that investors are overconfident. Build a mathematical model demonstrating the impact of overconfidence on the securities market.	Demonstrated that their model explained market volatility, overreactions, and then drift.
Fama (1998)	Studied whether the abnormal returns imply over- and under- reactions to information which refutes the efficient market hypothesis.	Found that anomalies are randomly split between over- and under- reactions, which is consistent with the efficient market hypothesis.
French and Roll (1986).	Researched why stock prices are more volatile during trading hours.	Private information is driving the volatility. The assumption is that informed investors have better access to private information and that they are more likely to trade during business hours.
Hayn (1989).	The authors hypothesized that losses have little information	Found evidence to support the hypothesis that losses less informative than profits about the firm's future prospects.

	value, because investors can liquidate the company.	
Kadiyala and Rau (2002).	Investigates two competing theories in behavioral finance: One which states that investors overreact to new information; the other which states investors underreact.	Investors tend to underreact to short-term information prior to the event itself and subsequentially to the information conveyed in the event.
Malkiel (2003).	Studied reported anomalies and predictable patterns in security prices which appear to challenge the efficient market hypothesis	Found that the anomalies and patterns are not robust or dependable in different sample periods; may be due to inaccurate assessments of risk, or do not offer superior returns after accounting for transaction costs.
Ramakrishnan and Tomash (1988).	Tested the relationship between earnings and stock price movements by dividing earnings into 3 categories: Permanent, Transitory, and Price-irrelevant.	Found that the model increased the explanatory value of earnings as measured by R-squared.
Savor (2012)	Analyzed stock performance after a major price change (defined as abnormal returns in excess of 10%).	Using analyst reports as a proxy for new information, found that investors underreact to news about a company's fundamentals and overreact to other shocks which move a firm's stock price.
Sprenger and Welpe (2011).	Studies whether the stock market reacts differently to different types of news events.	Market value differs based on the type of news. M&A and earnings announcement appear to have the largest effect. The absolute value of positive news prior to the news event is great than negative news, implying that positive news has a tendency to leak.
Staumbaugh, Yu, and Yang (2012).	Explores how market-wide sentiment combined with impediments to short-selling lead to anomalies. The impediments imply that there is only over-pricing.	Hypotheses were confirmed: Anomalies are stronger following high investor sentiment, returns on the short-leg (bottom 10% of stocks) is lowest after high investor sentiment (since they are the most overpriced), and overpricing on the long leg (top 10% of stocks) in minimal because they are the least overpriced.

Table 10: Interview questions

`

1. Information about the interviewee
    a. What is your current position?
    b. What are your major responsibilities?
    c. What do you enjoy most about your role?
    d. What are some of the challenges you face?
2. Information about the interviewee's news sources
    a. What sources do you use to get news on companies?
    b. Do you use social media, such as Twitter, for company news?
    c. Do you ever scan general internet sources (message boards, blog posts) for news and opinions about companies?
    d. Do you have a process for filtering noise from relevant news?
3. General questions about news events
    a. Are there any news categories (M&A, change in management, product launches, earnings, legal events, restructuring) that, on average, are more important to you than other events?
    b. How do you evaluate the significance of company news?
    c. How do you determine sentiment (bearish or bullish) when you see a news article?
    d. How do you determine the stock price significance of legal news (e.g., the company settled a lawsuit; announced that the company is the target of a lawsuit)?
4. Questions on data breaches/cybersecurity events
    a. Are you familiar with any recent data breach announcements?
        i. If so, did the breach news change your stock price forecast? Did you trade the security as a result of the news?
    b. How do you (or would you) evaluate the news of a data breach?
    c. How do you think consumers, in general, react to the news of a data breach?
    d. How do you think retail investors, in general, react to the news of a data breach?
    e. How do you think institutional investors, in general, react to the news of a data breach?
5. Is there anything that I didn't cover that you would like to add?

Table 11: Interviews

Interviewee	Role	Dates Interviewed
1,	Senior VP, investment management, insurance company	March 29, 2021
2.	Director, credit researcher, insurance company	April 21, 2021
3.	Technical trader	April 3, 2021 April 9, 2021
4.	Investments manager, insurance company. Focuses on bonds.	April 30, 2021
5.	Asset manager, insurance company	May 4, 2021
6.	Senior credit analyst, insurance company	May 4, 2021 May 10, 2021 May 12, 2021
7.	Risk manager, financial services company. Ex-investments manager for an insurance company.	June 2 , 2021
8.	Portfolio manager, investments firm.	June 2, 2021
9.	Investor relations manager, multiple companies	June 3, 2021
10.	Securities trader, investments firm	June 4, 2021
11.	Research analyst, investments firm	June 9, 2021
12	Retired portfolio manager, banking industry	June 10, 2021
13.	Investment manager, investments division of an insurance company	June 14, 2021
14.	Investment analyst, investments division of an insurance company	June 16, 2021 June 17, 2021
15.	Investor relations leader of an insurance company	June 21, 2021
16.	Vice President. Portfolio manager, high-wealth individuals.	June 24, 2021
17.	Senior investments leader.	June 30, 2021 July 2, 2021
18.	Co-founder and President, Capital Management Firm.	June 30, 2021

Table 12: Percentage of Fortune 1000 with Known Data Breaches

Source: Cyentia Institute

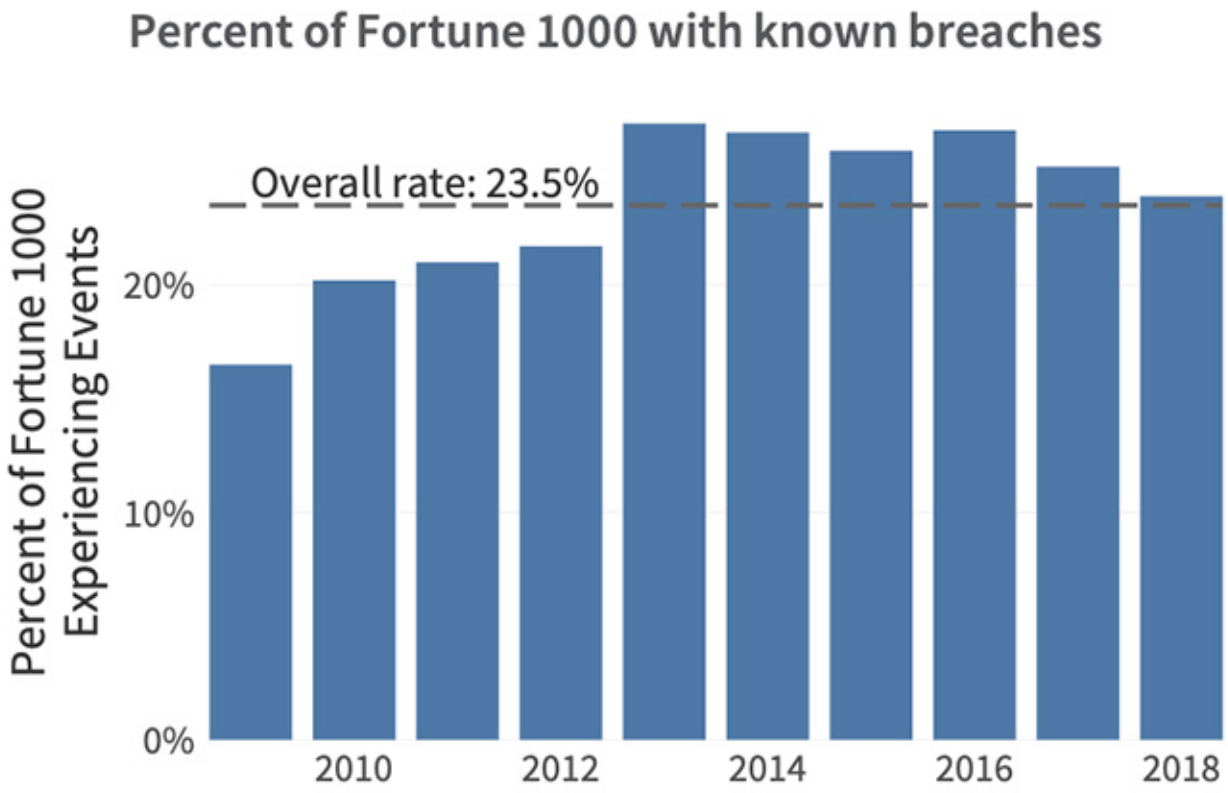
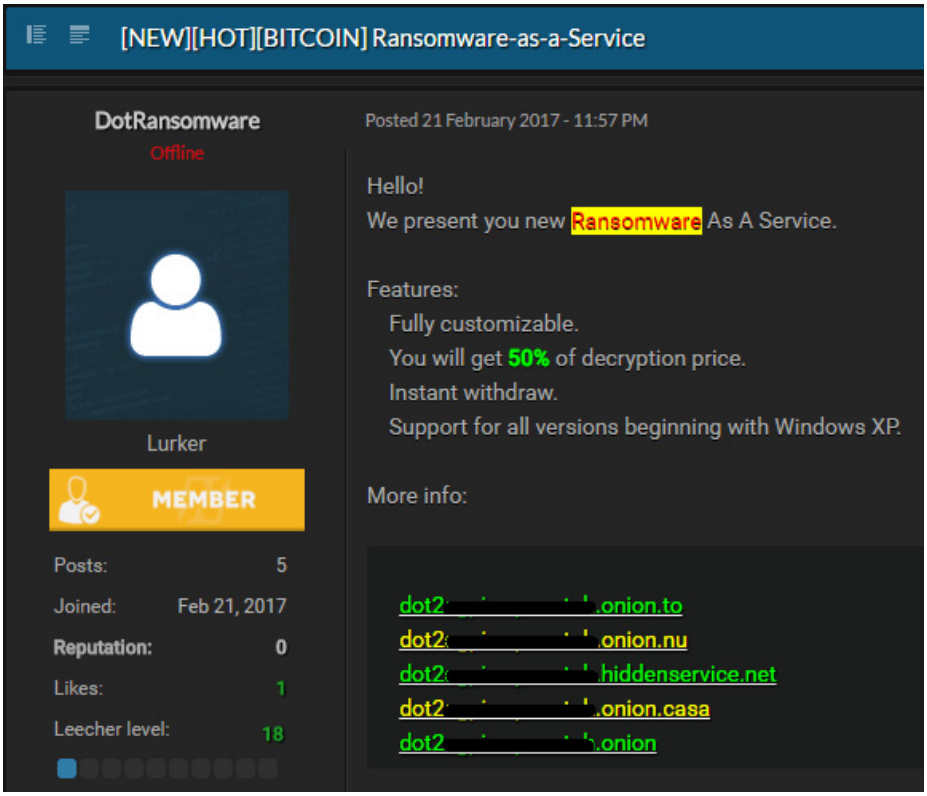


Table 13: Example Ransomware Advertisements



REFERENCES

Abrams, R (2017, May 23). *Target to Pay $18.5 Million to 47 States in Security Breach Settlement.* New York Times. https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488–500. https://doi.org/10.2307/1879431

Ali, S. E. A., Lai, F.-W., Hassan, R., & Shad, M. K. (2021). The Long-Run Impact of Information Security Breach Announcements on Investors' Confidence: The Context of Efficient Market Hypothesis. *Sustainability*, *13*(3), 1066. https://doi.org/10.3390/su13031066

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*, *41*(3), 893–916.

Aspan, M. (2017, September 8). *Why Equifax's Response Makes its Data Breach the Worst Ever.* Inc. Magazine. https://www.inc.com/maria-aspan/equifax-data-breach-worst-ever.html

Avast Security News Team (2021, May 21). *Insurer Against Ransomware Payments gets hit with ransomware.* Avast. https://www.insurancejournal.com/news/national/2021/07/07/621416.htm

Bajak, F (2021, July 7). *Cyber Insurance Industry in Crosshairs of Ransomware Criminals.* Insurance Journal. https://www.insurancejournal.com/news/national/2021/07/07/621416.htm

Baldassari, E. (November 11, 2018). Camp Fire death toll grows to 29, matching 1933 blaze as state's deadliest. *East Bay Times*.

Barbens, N., Shleifer, A., & Vishny, R. (1997). A model of investor sentiment. *Journal of Financial Economics*, *49*(3), 307-343.

Barber, B. M., & Odean, T. (2005). All that Glitters: The Effect of Attention and News on the Buying Behavior of Individual and Institutional Investors. *The Review of Financial Studies*. https://doi.org/10.2139/ssrn.460660

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Barrett, D. (2020, August 6). *Capital One fined $80 million for 2019 hack of 100 million credit card applications.* The Washington Post. https://www.washingtonpost.com/national-

security/capital-one-fined-2019-hack/2020/08/06/90c2c836-d7f3-11ea-aff6-220dd3a14741_story.html

Benaroch, M., & Chernobai, A. (2017). Operational IT Failures, IT Value Destruction, and Board-Level IT Governance Changes. *MIS Quarterly*, *41*(3), 729–762. https://doi.org/10.25300/misq/2017/41.3.04.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386. https://doi.org/10.2307/248684

Bessembinder, H. (Hank), Kahle, K. M., Maxwell, W. F., & Xu, D. (2005). Measuring Abnormal Bond Performance. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.650883

Bharadwaj, A. S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, *24*(1), 169. https://doi.org/10.2307/3250983

Bharadwaj, A., Keil, M., & Mähring, M. (2009). Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems*, *18*(2), 66–79. https://doi.org/10.1016/j.jsis.2009.04.001

Bing, C, Prentice, C, and Menn, J (2021, September 10). *Exclusive: Wide-ranging SolarWinds probe sparks fear in Corporate America.* https://www.reuters.com/technology/exclusive-wide-ranging-solarwinds-probe-sparks-fear-corporate-america-2021-09-10/

Bisson, D (2021, Nov 24). *Proposed Bill Would Require Public Disclosure of Ransomware Payments.* Security Intelligence. https://www.insurancejournal.com/news/national/2021/07/07/621416.htm

Black, J (2008). Forms and paradoxes of principles-based regulation. *Capital Markets Law Journal,* 3(4), 425-457. https://doi.org/10.1093/cmlj/kmn026

Boudoukh, J. (Kobi), Feldman, R., Kogan, S., & Richardson, M. P. (2012). Which News Moves Stock Prices? A Textual Analysis. *National Bureau of Economic Research*. https://doi.org/10.2139/ssrn.2193667

Brito, J & Watkins, T. (2011, April 24). Loving the cyber-bomb? The dangers of threat inflation in cybersecurity policy. Working Paper. Mercatus Center at George Mason University,

Bruton, G. D., Ahlstrom, D., & Li, H.-L. (2010). Institutional Theory and Entrepreneurship: Where Are We Now and Where Do We Need to Move in the Future? *Entrepreneurship Theory and Practice*, *34*(3), 421–440. https://doi.org/10.1111/j.1540-6520.2010.00390

Cain, C., Hanson, M., Ferber, S., & Johnson, W. (2021, August 1). *SEC Returns Spotlight to Cybersecurity Disclosure Enforcement*. The Harvard Law School Forum on Corporate Governance. https://corpgov.law.harvard.edu/2021/08/01/sec-returns-spotlight-to-

cybersecurity-disclosure-enforcement/

Campbell, K., Gordon, L. A., 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.

Cavusoglu, H., Mishra, B., & 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), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Chan, W., 2003, Stock Price Reaction to News and No-News: Drift and Reversal after Headlines. Journal of Financial Economics, 70, 223-260.

Cheng, X. (Joyce), & Walton, S. (2019). Do Nonprofessional Investors Care About How and When Data Breaches are Disclosed? *Journal of Information Systems*. https://doi.org/10.2308/isys-52410

Cimpanu, C. (2018, December 3). *Marriott sued hours after announcing data breach*. ZDNet. https://www.zdnet.com/article/marriott-sued-hours-after-announcing-data-breach/

Cognyte CTI Research Group (2021, August 8). *Ransomware Statistics 2021 – Growth and Analysis.* Cognyte. https://www.cognyte.com/blog/ransomware_2021/

Cooper, M. J., Gutierrez, R. C., & Hameed, A. (2004). Market States and Momentum. *The Journal of Finance*, *59*(3), 1345–1365.

Cooper, R.N, & Shiller, R. (2000). Irrational Exuberance. *Foreign Affairs*, *79*(4), 149.

Coveware (2021, October 21). *Ransomware Attackers down shift to 'Mid-Game' hunting in Q3 2021.* Coveware. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

Cruz, F. (2021, June 30). Ford Explorer Leads Segment in Sales during Q1 2021. *The Ford Authority.* https://fordauthority.com/2021/06/ford-explorer-sales-numbers-figures-results-first-quarter-2021-q1/.

Cutler, D. M., Poterba, J. M., & Summers, L. H. (1989). What moves stock prices? *The Journal of Portfolio Management*, *15*(3), 4–12. https://doi.org/10.3905/jpm.1989.409212

Damodaran, A. (1989). The Weekend Effect in Information Releases: A Study of Earnings and Dividend Announcements. *Review of Financial Studies*, *2*(4), 607–623. https://doi.org/10.1093/rfs/2.4.607

Daniel, K., Hirshleifer, D., & Subrahmanyam, A. (1998). Investor Psychology and Security Market Under- and Overreactions. *The Journal of Finance*, *53*(6), 1839–1885. https://doi.org/10.1111/0022-1082.00077

Data Breaches. (n.d.). Identity Theft Resource Center. Retrieved May 28, 2020, from https://www.idtheftcenter.org/data-breaches/?mod=article_inline

Deegan, C. (2002). Introduction: the legitimizing effect of social and environmental disclosures – a theoretical foundation. *Accounting, Auditing & Accountability Journal*, (15), 282-311.

Dey, D., & Zhang, G. (2014). Quality Competition and Market Segmentation in the Security Software Market. *MIS Quarterly*, *38*(2), 589–606. https://doi.org/10.25300/misq/2014/38.2.12

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147. https://doi.org/10.2307/2095101

Dynes, S, Goetz, E & Freeman, M (2013). Cyber security: Are economic incentives adequate? *International Conference on Critical Infrastructure*

Electronic Privacy Information Center. *Equifax Data Breach*. (2017) Electronic Privacy Information Center. https://epic.org/privacy/data-breach/equifax/

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, *272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

Equifax Data Breach. (2017) Electronic Privacy Information Center. Retrieved on https://epic.org/privacy/data-breach/equifax/

Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach. (2019, July 31). Federal Trade Commission. https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

Erazo, Felipe (2020, May 30). *Dark Web Merchants Sell Thousands of Stolen Credit Card Numbers*. (n.d.). Cointelegraph. Retrieved November 24, 2020, from https://cointelegraph.com/news/dark-web-merchants-sell-thousands-of-stolen-credit-card-numbers

Fama, E. F. (1970). Efficient Capital Markets: A Review of Theory and Empirical Work. *The Journal of Finance*, *25*(2), 383. https://doi.org/10.2307/2325486

Fama, E. F. (1998). Market Efficiency, Long-Term Returns, and Behavioral Finance. *Journal of Financial Economics 49*(1998) 283-306. https://doi.org/10.2139/ssrn.15108

Fama, E. F. & French, K.R. (1992). The Cross-Section of Expected Stock Returns. *The Journal of Finance*, *47*(2), 427-465.

Fama, E. F., & French, K. R. (1996). Multifactor Explanations of Asset Pricing Anomalies. *The Journal of Finance*, *51*(1), 55. https://doi.org/10.2307/2329302

Feiner, L. (2021, July 21). *New bill would make some companies report attacks to the government.* CNBC. https://www.cnbc.com/2021/07/21/new-bill-would-make-some-companies-report-cyber-attacks-to-government.html

Firth, M. (1976). The Impact of Earnings Announcements on the Share Price Behaviour of Similar Type Firms. *The Economic Journal*, *86*(342), 296. https://doi.org/10.2307/2230748

Fischer, E. (2014). *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*. https://sgp.fas.org/crs/natsec/R42114.pdf

Francia, A. (2020, February 24). *Capital One provides update on costs related to data breach, UK PPI reserve.* S&P Global Market Intelligence https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/capital-one-provides-update-on-costs-related-to-data-breach-uk-ppi-reserve-57229448

French, K.R., Roll, R.W., 1986. Stock return variance: the arrival of information and the reaction of traders. Journal of Financial Economics 19, 3–30.

Goldman, E., Rocholl, J., & So, J. (2008). Do Politically Connected Boards Affect Firm Value? *Review of Financial Studies*, *22*(6), 2331–2360. https://doi.org/10.1093/rfs/hhn088

Goldman, J. (2016, May 19). *52% of Consumers would pay more for products or services with Better Data.* eSecurityPlanet. https://www.esecurityplanet.com/networks/consumers-would-pay-more-for-products-or-services-with-better-data-security/

Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems*, *12*(9), 606–631. https://doi.org/10.17705/1jais.00275

Gomez, M. A & Whyte, C (2021). Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats. *International Studies Quarterly.* https://doi.org/10.1093/isq/sqab034

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach. *MIS Quarterly*, *41*(3), 703–727.

Gordon,L.A., Loeb, & Sohail. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, *34*(3), 567.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *19*(1), 33–56. https://doi.org/10.3233/jcs-2009-0398

Greenwald, J. (2020, September 4). *Cyber insurance premiums climbing rapidly: S&P.* Business Insurance. https://www.businessinsurance.com/article/20200904/NEWS06/912336487/Cyber-insurance-premiums-climbing-rapidly-S&P

Griffin, J. M., Harris, J. H., & Topaloglu, S. (2002). The Dynamics of Institutional and Individual Trading. *The Journal of Finance*. https://doi.org/10.2139/ssrn.316566

Hadar, M. (2011, September 11). Think your credit card is safe in your wallet? Think again. *Washington Post*. https://www.washingtonpost.com/business/think-your-credit-card-is-safe-in-your-wallet-think-again/2019/09/11/05e316e4-be0e-11e9-b873-63ace636af08_story.html

Haislip, J., Kolev, K., Pinsker, R., & Steffen, T. (2019). *The Economic Cost of Cybersecurity Breaches: A broad-based analysis*. Available at weis2019.econinfosec.org.

Hayn, C. (1995). The information content of losses. *Journal of Accounting and Economics*, *20*(2), 125–153. https://doi.org/10.1016/0165-4101(95)00397-2

Help Net Security. *Over 60% of the Fortune 1000 had at least one public breach over the last decade*. (2020, March 18). Help Net Security. https://www.helpnetsecurity.com/2020/03/18/fortune-1000-breach/

Henriquez, M (2021, September 20). *Banking industry sees 1318% increase in ransomware attacks in 2021.* Security Magazine. https://www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021

Henry, D. (2019, July 30). *Capital One customer data breach rattles investors.* Reuters. https://www.reuters.com/article/us-capital-one-fin-cyber-amazon-com/capital-one-customer-data-breach-rattles-investors-idUSKCN1UP1LD

HIPAA Journal. (2019, November 11). *HHS Increases Civil Monetary Penalties for HIPAA Violations in Line with Inflation*. HIPAA Journal. https://www.hipaajournal.com/hhs-increases-civil-monetary-penalties-for-hipaa-violations-2019-inflation/

Hoffman, C. (2021, May 10). *Ford Recalls 620,000 Explorers for Loose Roof Rail Covers*. Car and Driver. https://www.caranddriver.com/news/a36381768/ford-explorer-roof-rail-recall/

Hogan, K. M., Olson, G. T., & Angelina, M. (2020). A Comprehensive Analysis of Cyber Data Breaches and Their Resulting Effects on Shareholder Wealth. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3589701

Huang, K & Madnick, S. (2020, August 14). *A Cyberattack Doesn't Have to Sink Your Stock Price*. Harvard Business Review. https://hbr.org/2020/08/a-cyberattack-doesnt-have-to-sink-your-stock-price

Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017). Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks. *MIS Quarterly*, *41*(2), 497–523.

Ignatius, A. (2017, March-April). *We Need People to Lean into the Future.* Harvard Business Review. https://hbr.org/2017/03/we-need-people-to-lean-into-the-future

Jacob, J. (1997). Discussion of Do Security Analysts Improve Their Performance with Experience? *Journal of Accounting Research*, *35*, 159. https://doi.org/10.2307/2491459

Jegadeesh, N., & Titman, S. (1993). Returns to Buying Winners and Selling Losers: Implications for Stock Market Efficiency. *The Journal of Finance*, *48*(1), 65–91. https://doi.org/10.1111/j.1540-6261.1993.tb04702.x

Jegadeesh, N., & Titman, S. (2001). Profitability of Momentum Strategies: An Evaluation of Alternative Explanations. *The Journal of Finance*, *56*(2), 699–720. https://doi.org/10.1111/0022-1082.00342

Jewer, J., & McKay, K. (2012). Antecedents and Consequences of Board IT Governance: Institutional and Strategic Choice Perspectives. *Journal of the Association for Information Systems*, *13*(7), 581–617. https://doi.org/10.17705/1jais.00301

Johansmeyer, T. (2021, January 11). *Cybersecurity Insurance Has a Big Problem.* Harvard Business Review. https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem

Johnson, B. R. S. and Sidel, R. (2012, March 30). Data Breach Sparks Worry. *Wall Street Journal*.https://www.wsj.com/articles/SB10001424052702303816504577313411294908868

Joshi, A., Bollen, L., Hassink, H., De Haes, S., & Van Grembergen, W. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Information & Management*, *55*(3), 368–380. https://doi.org/10.1016/j.im.2017.09.003

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*, *28*(2), 275–301. https://doi.org/10.1108/ijaim-01-2019-0006

Kadiyala, P., & Rau, P. R. (2002). Investor Reaction to Corporate Event Announcements: Under-reaction or Over-reaction? *The Journal of Business, 77*(2), 357-386.. https://doi.org/10.2139/ssrn.312670

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2019.05.019

Kannan, K., Rees, J., & Sridhar, S. (2007). Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce*, *12*(1), 69–91. https://doi.org/10.2753/jec1086-4415120103

Kass. (2021, May 16). *French Insurer Axa Drops Ransomware Payment Coverage.* Managed Security Systems Provider. https://www.msspalert.com/cybersecurity-markets/europe/axa-drops-ransom-payment-coverage/

Kiemash, S, Brosen, L, and Steets, C. (2018, October 21). Cybersecurity Disclosure Benchmarking. *Harvard Law School Forum on Corporate Governance.* https://corpgov.law.harvard.edu/2018/10/21/cybersecurity-disclosure-benchmarking/#:~:text=While%20the%20U.S.%20Securities%20and

Kim, S. H., & Kwon, J. (2019). How Do EHRs and a Meaningful Use Initiative Affect Breaches of Patient Information? *Information Systems Research*, *30*(4), 1184–1202. https://doi.org/10.1287/isre.2019.0858

Kim, S. H., & Kim, B. C. (2014). Differential Effects of Prior Experience on the Malware Resolution Process. *MIS Quarterly*, *38*(3), 655–678. https://doi.org/10.25300/misq/2014/38.3.02

Korn, C. W., Sharot, T., Walter, H., Heekeren, H. R., & Dolan, R. J. (2013). Depression is related to an absence of optimistically biased belief updating about future life events. *Psychological Medicine*, *44*(03), 579–592. https://doi.org/10.1017/s0033291713001074

Kosseff, J. (2017). New York's financial cybersecurity regulation: Tough, fair, and a national mode. *Georgetown's Law Technology Review*, *1*(2), 436–445.

Kovar, J (2021, September 15). *SEC's SolarWinds Probe Could Expose Undisclosed Security Breaches: Report.* CRN. https://www.crn.com/news/security/sec-s-solarwinds-probe-could-expose-undisclosed-security-breaches-report

Krebs, B (2012, March 30). *MasterCard, VISA Warn of Processor Breach*. Krebs on Security https://krebsonsecurity.com/2012/03/mastercard-visa-warn-of-processor-breach/

Krebs, B. (2015, February 6). *China to Blame in Anthem Hack?.* Krebs on Security. https://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

Krebs, B (2017, September 8). *Equifax Breach Response Turns into a Dumpster Fire*. Krebs on Security. https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/

Kvochko, E., & Pant, R. (2015, March 31). *Why Data Breaches Don't Hurt Stock Prices*. Harvard Business Review. https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

Lam, W.M.M. & Seifert, J. (2021, July 31). Final Project Report: Regulatory Interactions and the Design of Optimal Cybersecurity Policies. *Digital Security by Design Social Science Hub*.

Lawson, S. (2013). Beyond Cyber-doom: Cyberattack scenarios and the Evidence of History. *Journal of Information Technology and Politics. 10*(1), 86-103. https://doi.org/10.1080/19331681.2012.759059

Lemnitzer J.M.. (2021). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy,* 1-19. https://doi.org/10.1080/23738871.2021.1880609

Lenard, T.M. and Rubin, P.H. (2006), "Much Ado about Notification". *Regulation 29*(44-50).

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

Li, Peters, Richardson, & Watson. (2012). The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Control Reports. *MIS Quarterly*, *36*(1), 179. https://doi.org/10.2307/41410413.

Liang, Y., & Telang, R. (2020). Customer Response to Adverse Security Events: An Empirical Study. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3523788

Limbert, F. (2019,, July 30). *Capital One shares diver after data breach affecting 100 million*. CNBC. https://www.cnbc.com/2019/07/30/capital-one-shares-dive-after-data-breach-affecting-100-million.html

Lumb, D. (2017, October 3). *Former Equifax CEO blames breach on one IT employee*. Engadget. https://www.engadget.com/2017-10-03-former-equifax-ceo-blames-breach-on-one-it-employee.html

Lunden, I. (2015, February 25). Target Says Credit Card Data Breach Cost It $162M In 2013-2014. *Techcrunch*. https://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14

MacColl, J, Nurse, J.C., and Sullivan, J. (2021, June 25). *Cyber Insurance and the Cyber Security Challenge.* Royal United Services Institute. https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge

MacKinlay, A. Craig. (1997). Event studies in economics and finance. *Journal of Economic Literature*, (35), 13-39.

MacKinney, N. (2020, July 7). *New research shows consumers want cybersecurity from service providers.* Cisco Umbrella. https://umbrella.cisco.com/blog/new-research-shows-consumers-want-cybersecurity-from-service-providers

Malkiel, B. G. (2003). The Efficient Market Hypothesis and Its Critics. *Journal of Economic Perspectives*, *17*(1), 59–82. https://doi.org/10.1257/089533003321164958

Masli, A., Richardson, V. J., Weidenmier Watson, M., & Zmud, R. W. (2016). Senior Executives' IT Management Responsibilities: Serious IT-Related Deficiencies and CEO/CFO Turnover. *MIS Quarterly*, *40*(3), 687–708. https://doi.org/10.25300/misq/2016/40.3.08

McGee, M. (2017, January 10). *A New In-Depth Analysis of Anthem Breach.* Bank Information Security. https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

Mele, C. (2018, August 1). Data Breaches Keep Happening. So Why Don't You Do Something? *The New York Times*. https://www.nytimes.com/2018/08/01/technology/data-breaches.html

Mello Jr, J (2021, November 23). *Many Consumers Fail to Protect Privacy After Receiving Data Breach Notice.* Technewsworld. https://www.technewsworld.com/story/many-consumers-fail-to-protect-privacy-after-receiving-data-breach-notice-87346.html

Meltzer, M. (2020, February 13). Equifax says data breach has cost it nearly $2 billion so far. *Atlanta Business Chronicle* .https://www.bizjournals.com/atlanta/news/2020/02/13/equifax-says-data-breach-has-cost-it-nearly-2.html

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology*, *83*(2), 340–363. https://doi.org/10.1086/226550

Miley, K. (2020, November 3). *OCC and HIPAA Cybersecurity Regulator Fines Now in Hundreds of Millions*. F5 Labs. https://www.f5.com/labs/articles/cisotociso/occ-and-hipaa-cybersecurity-regulator-fines-now-in-hundreds-of-m

Moldes, C. (2018, May 9). *Compliant but not Secure: Why PCI-Certified Companies Are Being Breached.* Cybersecurity and Information Systems Information Analytics Center. https://csiac.org/articles/compliant-but-not-secure-why-pci-certified-companies-are-being-breached

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311.

Moore, T. (2010). The economics of cybersecurity: Principles and Policy options. *International Journal of Critical Infrastructure Protection. 3*(3-4), 103-117. https://doi.org/10.1016/j.ijcip.2010.10.002

Moreno, J. (2017, October 13). *States Respond to Equifax Cyber Breach with Enforcements Actions and Calls for Enhanced Regulatory Powers.* Cadwalader, Wickersham, and Taft LLP. https://www.jdsupra.com/legalnews/states-respond-to-equifax-cyber-breach-59577/

Morgan, B. (2020, June 22). *50 Stats Showing Why Companies Need to Prioritize Consumer Privacy.* Forbes. https://www.forbes.com/sites/blakemorgan/2020/06/22/50-stats-showing-why-companies-need-to-prioritize-consumer-privacy/?sh=61c1f1737f61

Morse, E. A., Raval, V., & Wingender, J. R. (2011). Market Price Effects of Data Security Breaches. *Information Security Journal: A Global Perspective, 20*(6), 263–273.

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for Cybersecurity. *Daedalus*, *140*(4), 70–92. https://doi.org/10.1162/daed_a_00116

Myers, M.D. (2020). *Qualitative Research in Business & Management.* Sage Publications Ltd.

Myers, M.D. & Newman. (2007). The Qualitative Interview in IS research: Examining the craft. *Information and Organization, 17*(1), 2-26.

Newman, L. (2017, October 3). *6 Fresh Horrors from Equifax CEO Richard Smith's Congressional Hearing*. WIRED. https://www.wired.com/story/equifax-ceo-congress-testimony/

Nimalendran, M. (1994). Estimating the Effects of Information Surprises and Trading on Stock Returns Using a Mixed Jump-Diffusion Model. *Review of Financial Studies*, *7*(3), 451–473. https://doi.org/10.1093/rfs/7.3.451

Nolan, R, and McFarlan, F (2005, October). Information Technology and the Board of Directors. *Harvard Business Review*.

O'Donoghue, T., Rabin, M. (1999). Doing it now or later. *American Economic Review 89*(1), 103-124. https://doi.org/10.1257/aer.89.1.103

Oliver, C. (1991). Strategic Responses to Institutional Processes. *The Academy of Management Review*, *16*(1), 145. https://doi.org/10.2307/258610

O'Reilly, K., Paper, D., & Marx, S. (2012). Demystifying Grounded Theory for Business Research. *Organizational Research Methods*, *15*(2), 247–262. https://doi.org/10.1177/1094428111434559

Popken, B. (2017, October 5). *Former Equifax CEO Blames One IT Guy for Massive Hack.* ABC News. https://www.nbcnews.com/business/consumer/former-equifax-ceo-blames-one-it-guy-massive-hack-n807956

Rabinowitz, R. (2020). From Securities to Cybersecurity: The SEC Zeroes in on Cybersecurity. *Boston College Law Review 61*(4), 1534-1575.

Ramakrishnan, R. T. S., & Thomas, J. K. (1998). Valuation of Permanent, Transitory, and Price-Irrelevant Components of Reported Earnings. *Journal of Accounting, Auditing & Finance*, *13*(3), 301–336. https://doi.org/10.1177/0148558x9801300309

Richardson, V., Watson, M. W., & Smith, R. E. (2019). Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems*.

Riddick, S. (2021, September 8). The SEC is Serious About Cybersecurity. Is Your Company? *Harvard Business Review*. https://hbr.org/2021/09/the-sec-is-serious-aboutcybersecurity-is-your-company

ROKKEX. (2019, December 3). *Data Breaches: Why We Don't Even Care Anymore*. Medium. https://medium.com/@rokkex/data-breaches-why-we-dont-even-care-anymore-eed75cfb0cfb

Rotenberg,W. (2017, September 26). *Equifax, the Credit Reporting Industry, and what Congress should do next.* The Harvard Business Review. https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next

Sambamurthy, Bharadwaj, & Grover. (2003). Shaping Agility through Digital Options: Reconceptualizing the Role of Information Technology in Contemporary Firms. *MIS Quarterly*, *27*(2), 237. https://doi.org/10.2307/30036530

Savor, P. G. (2012). Stock returns after major price shocks: The impact of information. *Journal of Financial Economics*, *106*(3), 635–659. https://doi.org/10.1016/j.jfineco.2012.06.011

Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information and Computer Security*, *24*(1), 73–92. https://doi.org/10.1108/ics-03-2014-002

Science and Technology Committee, "Personal Internet Security", House of Lords, Science and Technology Committee, 5th report of Session 2006-07, HL Paper 165-I, 2007.

Schneier, A & Arnold, C. (2019, July 22). *Equifax to Pay Up to $700 Million In Data Breach Settlement.* NPR. https://www.npr.org/2019/07/22/744050565/equifax-to-pay-up-to-700-million-in-data-breach-settlement.

Schneier, B. (2001, February). *The Insurance Takeover.* Schneier on Security. https://www.schneier.com/essays/archives/2001/02/the_insurance_takeov.html

Schroeder, P. (2020, October 8). Citigroup fined $400 million by regulators, agrees to fix "longstanding deficiencies." *Reuters*. https://www.reuters.com/article/usa-citigroup-enforcement/citigroup-fined-400-million-by-regulators-agrees-to-fix-longstanding-deficiencies-idUSKBN26T0BL

Seals, T. (2021, August 3). *Ransomware Volumes Hit Record Highs as 2021 Wears On.* Threatpost. https://threatpost.com/ransomware-volumes-record-highs

Shapiro, S. P. (2005). Agency Theory. *Annual Review of Sociology*, *31*(1), 263–284. https://doi.org/10.1146/annurev.soc.31.041304.122159

Sharma, A. (2018, September 27). *What Chegg's Database Breach Means for Its Stock*. The Motley Fool. https://www.fool.com/investing/2018/09/27/what-cheggs-database-breach-means-for-its-stock.aspx

Sharot, A. (2011). The optimism bias. *Current Biology, 21*(23), R941- R945. https://doi.org/10.1016/j.cub.2011.10.030

Smith, J. A., Rom Harré, & Luk Van Langenhove. (1995). *Rethinking methods in psychology*. Sage Publications.

Song, V., Cavusoglu, H., Lee, G., & Ma, M. (2020). IT Risk Factor Disclosure on Stock Price Crashes. *Proceedings of the 53rd Hawaii International Conference on System Sciences*. http://hdl.handle.net/10125/64480

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, 216–229. https://doi.org/10.1016/j.cose.2015.12.006

Sprenger, T. O., & Welpe, I. M. (2011). News or Noise? The Stock Market Reaction to Different Types of Company-Specific News Events. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1734632

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, *92*, 178–188. https://doi.org/10.1016/j.future.2018.09.063

Stambaugh, R.F., Yu, J, and Yuan, Y. (2012). The short of it: Investor sentiment and anomalies.

Journal of Financial Economics 104, 282-302.

Stempel, J., & Bose, N (2015, December 3). Target in $39.4 million settlement with banks over data breach. *Reuters*. https://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203

Suchman, M.C. (1995) Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review 20*, 571-610.

Suddaby, R. (2006). From the Editors: What Grounded Theory is Not. *Academy of Management Journal*, *49*(4), 633–642. https://doi.org/10.5465/amj.2006.22083020

Swinhoe, D. (2020, January 31). The biggest data breach fines, penalties and settlements so far. *CSO Online*. https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html?page=2

Telang, R., & Wattal, S. (2007). An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price. *IEEE Transactions on Software Engineering*, *33*(8), 544–557. https://doi.org/10.1109/tse.2007.70712

Temple-Rason, D (2021, April 16). *A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack.* NPR. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

Tolbert, P.S. Zucker, L.G. (1996). The Institutionalization of Institutional Theory. *Handbook of Organization Studies*, 175–190.

U.S. Securities and Exchange Commission (2018, February 26). *Commission Statement and Guidance on Public Cybersecurity Disclosures.* Available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf

U.S. Securities and Exchange Commission (2021, June 15). *SEC Charges Issuer with Cybersecurity Disclosure Controls Failures.* Available at: https://www.sec.gov/news/press-release/2021-102.

Van Der E & Lee, T. B. (2015, January 20). *The 2014 Sony hacks, explained*. Vox; https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

Verizon (2020, October 6). *2020 Payment Security Report.* Verizon Business Resources. https://www.verizon.com/business/resources/reports/payment-security-report/

Vincent, N. E., Higgs, J. L., & Pinsker, R. (2018). Board and Management-Level Factors Affecting the Maturity of IT Risk Management Practices. *Journal of Information Systems*. https://doi.org/10.2308/isys-52229

Volz, D & Shepardson, D. (2017, September 8, 2017). *Criticism of Equifax breach response mounts, shares tumble.* Reuters https://www.reuters.com/article/us-equifax-

cyber/criticism-of-equifax-data-breach-response-mounts-shares-tumble-idUSKCN1BJ1NF

Wade, M and Hulland, J. (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. *MIS Quarterly*, *28*(1), 107. https://doi.org/10.2307/25148626

Walton, R (2021, April 15). *NERC Finding 25% of utilities exposed to SolarWinds hack indicates growing ICS vulnerabilities, analysts say.* Utility Dive. https://www.utilitydive.com/news/nerc-finding-25-of-utilities-exposed-to-solarwinds-hack-indicates-growing/598449/

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The Association Between the Disclosure and the Realization of Information Security Risk Factors. *Information Systems Research*, *24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly*, *39*(1), 91–112.

Wang, R. (2020, May 28). *How to Lead a Data-Driven Digital Transformation*. Harvard Business Review. https://hbr.org/webinar/2020/05/how-to-lead-a-data-driven-digital-transformation

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal*, *5*(2), 171–180. https://doi.org/10.1002/smj.4250050207

Westerman, G. (2014, June 12). *The Nine Elements of Digital Transformation*. Harvard Business Review. https://hbr.org/webinar/2014/06/the-nine-elements-of-digital-transformation

White, J (2021, October 7). *Ransomware as a Service: Criminal "Entrepreneurs" Evolve Ransomware.* Palo Alto Networks. https://www.paloaltonetworks.com/blog/2021/10/ransomware-as-a-service/

Whittaker, Z (2018, December 10). *Equifax breach was 'entirely preventable' had it used basic security measures, says House report.* TechCrunch. Retrieved from https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/#:~:text=The%20credit%20agency%20failed%20to

Whittaker, Z (2019, July 22). *FTC Slaps Equifax with a fine of up to $700M for 2017 data breach.* TechCrunch. Retrieved from https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/#:~:text=The%20credit%20agency%20failed%20to

Wider, J. (2021, October 12). *New U.S. Bill Would Require Disclosure of Ransomware Payments.* Healthcare Innovation. https://www.hcinnovationgroup.com/cybersecurity/news/21241982/new-us-bill-would-require-disclosure-of-ransomware-paymentsWamsley, L. *Ohio House Speaker Arrested*

In Connection With $60 Million Bribery Scheme. (2020, July 21). NPR.org. https://www.npr.org/2020/07/21/893493224/ohio-house-speaker-arrested-in-connection-to-60-million-bribery-scheme

Wu, S. P.-J., Straub, D. W., & Liang, T.-P. (2015). How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and IT Managers. *MIS Quarterly*, *39*(2), 497–518. https://doi.org/10.25300/misq/2015/39.2.10

Yayla, A. A., & Hu, Q. (2011). The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors. *Journal of Information Technology*, *26*(1), 60–77. https://doi.org/10.1057/jit.2010.4

Zetter, K. (2012, April 2). *Global Payments Says 1.5 Million Cards Stolen; Won't Discuss Details of Breach*. Wired. https://www.wired.com/2012/04/global-payments-breach/