Fall 11-18-2016

# Cybercrime Effects on Stock Prices

Amie Jones

Amie Jones

Murray State University Honors Program

HONORS THESIS

Certificate of Approval

Cybercrime Effects on Stock Prices

Amie Jones

May 2017

Approved to fulfill the
requirements of HON 437

_____

Dr. Murphy Smith,
Dill Distinguished Professor
Accounting

Approved to fulfill the
Honors Thesis requirement
of the Murray State Honors
Diploma

_____

Dr. Warren Edminster,
Executive Director
Honors College

Examination Approval Page

Author: Amie Jones

Project Title: Cybercrime Effects on Stock Prices

Department: Accounting

Date of Defense: November 18, 2016

Approval by Examining Committee:

_____ _____
(Dr. Murphy Smith, Advisor) (Date)

_____ _____
(Dr. Leigh Johnson, Committee Member) (Date)

_____ _____
(Dr. Katherine Smith, Committee Member) (Date)

# Cybercrime Effects on Stock Prices

Submitted in partial fulfillment
of the requirements
for the Murray State University Honors Diploma

Amie Jones

May 2017

Table of Contents

List of Illustrations/Figures/Tables

Senior Honors Thesis Prospectus—Proposed Study Abstract

Author: Amie Jones

Advisor: Dr. Murphy Smith

Projected Date of Completion: November 11, 2016

Cybercrime is a prevalent and serious threat to publicly traded companies. This rapid growing crime is referred to as "the greatest transfer of wealth in human history" or the "rounding error in a fourteen trillion-dollar economy." Cybercrime costs companies billions of dollars through stolen assets or lost business and creates a permanent blemish to the companies' reputation. After the announcement of cybercrime in a company, customers begin to worry about the security of their financial transactions. Known history or an announcement of cybercrime within the company can ultimately lead to lower stock prices or lost business. Lowered stock prices and lost business become legitimate concerns of financial analysists, investors, and creditors. This thesis examines multiple case studies which demonstrates the impact of cybercrime on stock prices, marketing activities and actions, and stockholder value. The case studies will examine the different types of cybercrime and its consequences to the company. Thus, this thesis provides a in depth analysis of how cybercrime or its announcement of weak cyber security affects stock prices in a company, the attitudes toward cybercrime from stockholders, and the need for businesses to increase their security programs to prevent future attacks.

Approval:

| | |
|---|---|
| _____ | _____ |
| (Dr. Murphy Smith, Advisor) | (Date) |
| _____ | _____ |
| (Dr. Don Chamberlain, Chair) | (Date) |
| _____ | _____ |
| (Dr. Warren Edminster, Honors College Director) | (Date) |

# Cybercrime Effects on Stock Prices

## INTRODUCTION

The development and use of the computer and the internet have created countless possibilities and benefits for businesses including e-commerce, faster transactions, better communication, and increased marketing and publicity. These advantages have created opportunities for growth and expansion for businesses worldwide. However, these benefits also come with a heavy cost of potential threats to security. Cybercrime is an ever growing and prevalent threat to publicly traded companies. Cybercrime costs businesses potentially millions of dollars annually in prevention, stolen assets, lost business, and can create a permanent blemish to a company's reputation. An erroneous or fraudulent transaction can be completed quickly with a click of a button, which can be costly to find and to correct the damage.

Cybercrime is an ongoing concern because if shareholders are not confident in a company's cyber security and internal control, they will move their investment capital. In addition, companies can lose business if they are perceived to be targets of cybercrime. Their market value may decrease as a result of lost business. This thesis examines cybercrime, its threat, and its effect on publicly traded companies' stock prices. This study analyzes ten case studies of highly publicized cybercrime, affecting publicly traded companies. The research questions addressed by this thesis include: 1) How does cybercrime news stories affect stock prices in publicly traded companies? 2) How does this impact affect everyday consumers?

## LITERATURE REVIEW

The invention of the first electronic computer in 1946 was considered a breakthrough in processing technology and created a pathway to new opportunities for communication and business. Not long after the first use of electronic data interchange, the first record of cybercrime

was committed. According to Norton Security Symantec Corporation, cybercrime is a “crime that has some kind of computer or cyber aspect to it" (Norton, 2016, p. 1). The first account of cybercrime occurred in 1970 and involved a teller at the New York’s Dime Savings Bank who used a computer to embezzle over $2 million (Wavefront, 2016). Eight years later, the first spam email was sent over ARPAnet, the US Defense Department network, by a Digital Equipment Corporation marketing executive. (Julien, 2016). The use of cybercrime through dishonest use of computer access to information or programming has exploded since the 1900s. While the use of the computer and its capabilities rose, so did attacks on computer systems. Threats have grown from minor attacks to large-scale cybercrime activity. Table 1 shows the timeline and evolution of cybercrime to present day.

[See Table 1: Timeline of Cybercrime]

Cybercrime has many incentives for hackers. Cybercrime produces high returns at low risk and a relatively low cost for the hacker. Unlike the other types of crime, cybercrime allows hackers to hide behind computer screens and not have physical confrontation. The incentive to steal more is irresistible for hackers and creates a potential for almost instant personal gain with the click of a button. Hackers have economical, personal, ideological, and structural motivations to commit cybercrime. Money is a large motivation for crime with today’s pressure to get ahead or get rich in life. Hackers also see the opportunity for personal gain and to carry out personal vendettas. Cybercriminals also make a profit for selling stolen information on the Black Market. On an international scale, cybercrime has been committed by foreign governments to retaliate against United States actions. The attackers do not view cybercrime as a crime, but as a sneaky opportunity to get ahead. Hackers pinpoint and choose their victims strategically and look for points of weakness in the target (Smith et al. 2003).

Hackers view both the average person as well as publicly traded companies as targets. The average person is an easy target because more and more people use technology. “With more and more people using the internet to store personal information, there is increasing potential for personal information rewards” (Mercer, 2016, p. 1). Many people do not check the security of networks, neglect the protection of their everyday software with passcodes, and use personal information for shopping over the internet. Often times, people disregard the safety of their transactions and avoid taking preventive measures altogether. Any transactions involving a computer or ecommerce provide hackers with sensitive information that can be retrieved if the data was hacked (Mercer, 2016).

In regards to cybercrime in publicly traded companies, retail stores and healthcare tend to be popular targets for cybercrime activity. Both retail stores transactions and healthcare records provide a numerous amount of personal information that can be retrieved on a large scale rather than each individual person. Millions of people are involved so it becomes a popular target for hackers. According to ITBusinessEdge, retail stores are a prime target for attackers because they use a multi-channel strategy that spreads personal data across multiple locations making monitoring difficult. POS or point-of-sale terminals are easy targets for hackers who use encryption to retrieve data. Data is obtained as the customer swipes their cards through a reader. QR codes or quick response codes are easily manipulated which can potentially contain personal information. Transitions between old and new technology or systems for retail stores create a gap of time for hackers to find a loophole in the system. New “tap-to-pay” or “mobile wallets” create risk because retailers cannot as easily monitor who can access the system (ITBusinessEdge, 2016).

Healthcare is also another popular target for cybercriminals. Healthcare has not been very secure in the past. In 2009, Congress passed HITECH which is the Health Technology for Economic and Clinical Health Act which required hospitals to switch from paper to electronic health records. This transition created the opportunity to obtain new health information and personal information. Healthcare often also uses out of date internet browsing which can create more opportunities for attacks (ITBusinessEdge, 2016).

Though large retail stores and healthcare tend to be popular victims, other business are still targets regardless of size. According to Microsoft, 20% of small to mid-sized businesses have been targets of cybercrime attacks (Morgan, 2016). This proves that the size of a business nor the service makes it immune to hackers. Businesses and individuals must determine the amount that they are willing to spend to reduce the risk and the potential loss. The saying, "prevention is expensive, but is cheaper than the treatment" applies to the case of cybercrime because its effects can be detrimental. The problem especially arises if companies are not fully aware of their potential losses or underestimate their vulnerability, while also underestimating risk.

There are numerous types of cybercrime. Types of cybercrime are continually evolving and expanding. This demands more costs to protect data and more research to prevent cyberattacks. Table 2 shows the common types of cybercrime that are used to attack computers.

[See Table 2: Common Types of Cybercrime]

## ECOMMERCE AND RISK

Today, ecommerce is a common and convenient way to handle transactions. Ecommerce is defined as commercial transactions conducted electronically over the internet. According to Smith, the internet is "widely used for both business-to-business (B2B and business-to-consumer (B2C) transactions." B2B ecommerce describes the electronic commerce between businesses at the level of manufacturers, wholesalers, and retailers as opposed to between companies and the general public or government. B2C ecommerce is defined as the business of transactions conducted directly between a company and consumers who are the end-users of its products or services (Statista, 2016). Transaction and communication is almost instant as well as very convenient for both parties.

Ecommerce has a value of $1.5 trillion dollars and it approximately mades up 18% of the entire merchant wholesale trade in 2011. In 2013, global B2C ecommerce sales reached $1.2 trillion dollars and 29.7% was generated by the United States (Statista, 2016). Ecommerce continues to grow by expanding to 198 million US shoppers in 2014 which is approximately 78% of the entire population. According to the US Census Bureau, ecommerce factored to be 7.5% of all retail in the US for the fourth quarter of 2015. This represents a .5% growth from the first quarter to the fourth quarter (ReadyCloud, 2016).

## THREATS TO COMPUTER SECURITY

There are numerous threats associated with cybercrime that pose risks to businesses and individuals. In the past, individuals or small groups mainly committed cybercrime, but it is now highly complex and involves numerous individuals across the world to commit crimes on an unprecedented scale (Interpol, 2016). The workplace environment has evolved into a highly dynamic system with a mobile workforce. The use of mobile transactions also opens up new

doors to potential hacks. Workers no longer stay within the confines of a trusted network so this can make security more difficult.

The use of the cloud for more storage control and management opens a new way to store data, but also provides hackers a new opportunity to try to obtain information. Malware is still a common threat, but there is a shift towards new threats. These include fileless attacks, exploits of remote shell and remote control protocols, encrypted infiltrations and credential theft (McAfee, 2016). A main concern is hijacking from remote computers to take control of a system, enabling the installation of malicious codes. Other potential risks involve the following (Smith et al. 2003, p. 2):

- "The changing e-business environmental alters the risks, so old solutions may no longer work.
- International business activity expands the scale and scope of risks.
- Computer power, connectivity, and speed can spread viruses, facilitate system compromise, and compound errors in seconds potentially affecting interconnected parties.
- Hackers never stop devising new techniques; thus, new tools mean new vulnerabilities.
- Digitization creates unique problems for digital information and transactions."

Technology is ever improving, but there will always be new ways to hack into new devices. With more technology, comes a stronger need for security to ensure the safety of businesses and individulas.

## COSTS OF CYBERCRIME

Businesses must determine the amount that they are willing to spend to reduce the risk and the potential loss. The costs include repair costs, recovery costs, lost business, and the potential of shutting business altogether to solve the cybercrime crisis. The costs of cybercrime continue to grow year to year. Many cases of cybercrime go unreported so it is difficult to put an exact number on losses of cybercrime. In 2011, cybercrime costs businesses on average $9 billion. In 2015, the total cost of cybercrime for businesses in the United States economy was over $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business. For 2016, losses are estimated between $375 billion to $575 billion. Even the smallest of these figures is more than the national income of most countries (McAfee, 2016). Cybercrime costs are projected to reach $2 trillion by 2019 (Morgan, 2016).

The most important cost of cybercrime is the damage to the company's reputation and to national economies. Customers lose faith in businesses if they feel that their personal information and transactions are not secure. With telecommunications, breaches of cybercrime are announced through radio, television broadcasts, and social media. Those records are documented for years, which places a blemish on the reputation of the business. Cybercrime damages trade, competitiveness, innovation, and global economic growth. The costs of cybercrime will continue to increase as more businesses shift their operations online and more consumers connect to the internet. Losses on the theft of intellectual property will also increase as other countries improve their ability to make use of it to manufacture competing goods at lower costs. Cybercrime slows the pace of global innovation by reducing the rate of return to innovators and investors (McAfee, 2016).

**PROCEDURE**

The procedure's model for the following case studies was previously used in a study by Smith et al. (2003). Publicly traded companies were researched for the earliest announcement date of cybercrime in the company within the past ten years. An Excel sheet was created to organize the data including the ticker symbol, the type of cybercrime committed, targeted information, victims, perpetrator, impact, cost, response of the targeted company, date of the article, and the percent change in the company stock price. Stock prices were retrieved from Yahoo Finance under historical lookup dates.

The market price was recorded for a week before the announcement, three days before, the day of the announcement or release of the article, three days after, and a one week after. Stock prices were used on the most accurate date according to the seven, three, and one day before and after the attack. For example, if the stock market was closed a week before the announcement of cybercrime, the next available day the stock was traded was used for the analysis.

A formula was used in Excel to create the data resulting in the percent change in the company stock price per day. The percentage of change reflects the amount of change from Day 0 which is the day of the cybercrime attack announcement. The percentage change in the stock price was then compared to the Dow Jones Industrial average to determine whether the stock price increased or decreased along with the rest of the market or if the news announcement might have been independently affected in the increase or decrease of the company's stock price. A T-Test was used to determine the whether there was a significant difference in the stock price changes as compared to changes in the Dow Jones Industrial Index.

## CASE STUDIES

Following are case studies of 10 publicly traded companies. Details of each case are provided. The companies are listed in Table 3.

[See Table 3: Companies and Cybercrime]

## CITIGROUP

On June 16, 2011, Citigroup, an investment banking and financial service, announced that they had fallen victim to a cybercrime attack. A group called Lulzsec cracked into the bank's vast reservoir of personal information and used malware to retrieve names, account numbers, contact information, social security numbers, card expiration dates, and CVV. Hackers logged onto the site reserved for credit card users and inserted various account numbers into a string of text located in the address bar. The code systems repeated this processes allowing them to capture confidential information. Though this method seemed simple, the hackers knew how to breach security by pinpointing their vulnerability. They were detected during a routine check in early May (Dash and Schwartz, 2011).

There were 360,000 accounts affected and 1% of those accounts were North American. The number of accounts affected were 80% more than first estimated. This ultimately cost Citigroup $2.7 million in repairs. Citigroup reissued customers with new cards with a notification letter and customers were not liable for transactions with suspected fraud. However, Citigroup was criticized for not offering customers a full year of Preventive credit file monitoring services which is the standard for large companies having suffered similar attacks (Dash and Schwartz, 2011).

**TARGET**

On December 19, 2013, Target Corporation announced a breach in its cyber security. This was especially devastating to customers because the breach happened during the holiday season. There was an estimated of 40 million accounts hacked, but there were 70 million accounts affected. Accounts fell victim to a POS/KAPTOXA cybercrime committed by Daniel Dominguez Guardiola and Mary Carmen Vaquera Garcia. Target's customers' credit and debit card names, expiration dates, and CVV were sold on the black market for $53.7 million (Tobias, 2015).

The malware began collecting data as soon as it infected the retailer's POS terminals, but stayed under the radar for six days. According to McAfee, "The attackers were able to plant point-of-sale malware and intercept approximately 110,000,000 records worth of payments, transactions, and other personally identifiable data (Rashid, 2014)." This cost Target $148 million dollars which included payment for one year of free credit monitoring and identity theft. The company spent $61 million in anti –breach technology after the attack and profits fell 46% in the fourth quarter of 2013 (Tobias, 2015). Because of the incident, Target lowered its fourth quarter earnings in 2013 and share price to fell $.10 per share with a sales decline of 2% to 6% in the period following the announcement of the data breach (Rashid, 2014).

This caused enormous damage to Target's reputation and stock prices, and, ultimately, Beth M. Joacob, Senior Technology Officer, and Gregg Steinhafel, CEO and Chairman, both resigned from their job after the attack. Target executives were summoned to appear before congressional panels about data privacy. The executives admitted that they had ignored warnings signs about security gaps. Memos by the federal government and research firms suggested that new malware was targeting the payment system which allowed too much access to vendors. This

security breach also moved the timetable of the announcement of the new chip and pin system for credit and debit cards for preventive measures for customers (Rashid, 2014).

**ANTHEM**

Anthem, Inc. defines itself as a company who is "working to transform health care with trusted and caring solutions…With more than 73 million people served by its affiliated companies including nearly 40 million enrolled in its family of health plans, Anthem is one of the nation's leading health benefits companies" (Anthem, 2016). Anthem is the second largest health insurer in the United States and owns Blue Cross Blue Shield (Matthews, 2015). On January 29, 2014, Anthem announced that their database was hacked which included the personal information for 78.8 million people (60 million to 70 million of its own current and former customers and employees). Joseph Swedish, Anthem president and CEO stated, "Anthem was the target of a very sophisticated external cyber attack" (Weise, 2015). This cybercrime involved malware used by a group in China called the Black Vine (Paganni, 2015).

Data was obtained from customers as far back as 2004 (Matthews, 2015). The data obtained included names, date of birth, medical IDs, Social Security numbers, street addresses, email addresses, employment information, and income data. According to USA TODAY, no credit card information was obtained. Because no medical information was obtained, the breach did not come under HIPAA rules, which governs the security of medical information. This incident cost Anthem $148 million and was deemed the largest healthcare breach to date. Victims were notified with a letter of apology explaining the situation including identity protection services such as AllClear ID protection for two years at no cost. Credit monitoring and child identity protection was also issued to customers. The letter also included Preventive

measures such as a toll-free hotline, fraud protection tips, and credit freeze information (Weise, 2015).

**MICHAELS COMPANIES.**

Michael's Corporation is a 40-year-old North American arts and crafts retail chain that operates approximately 1,200 stores. Michael's has been under attack on its cyber security on more than one occasion. In 2011, Michael's issued a statement saying that their debit card processing equipment had been tampered with in approximately 80% of the stores. At the time, it uncovered improperly altered PIN pads that allowed hackers to skim debit cards and steal personal data to create duplicate cards. Some credit card information had also been processed and had replaced 7,200 PIN pads (Dowell, 2014).

However, the attack announced on April 4, 2014 was on a much larger scale. There were 3 million customers affected. Michael's first acknowledged the breach in January, not long after the attack on Target. A statement released by Michael's which stated that the computer hack involved "highly sophisticated malware that had not been encountered previously by either of the security firms" (Harris, 2014, p. 1). The group suspected was a band of criminals located in Eastern Europe. Customers' payment card information, card numbers, and expiration dates were hacked. Michael's issued a letter of apology from the CEO and offered a hotline to report suspected fraud. Aaron Brothers, a framing sister store to Michael's, confirmed that between June 26, 2013 and February 27, 2014, 54 Aaron Brothers stores were affected by malware. There were approximately 400,000 cards that were potentially impacted during this period. The company's highest ranking technology executive, Beth M. Jacob, resigned from her position (Harris, 2014).

## UNIVERSAL CONTINENTAL HOLDINGS, INC.

Universal Continental Holdings, Inc., which owns United Airlines, announced its attack on July 29, 2014. United Airlines is the second largest airline. Passenger flight information and destination information and Social Security numbers from the Office of Personal Management were stolen. This data could also be cross-referenced with stolen medical and financial records. There were 21.5 million accounts hacked and 80% of victims were from the United States. The theft of airline records potentially adds another layer of information that could allow the perpetrator to chart the travel patterns of specific government or military officials. Unlike health records or financial data, the breach of airlines raises concerns by exposing access to the movement of millions of passengers (Riley and Robertson, 2015).

The suspected perpetrators were the Chinese group, called the Black Vine which was also connected to the Anthem attack. This group has been linked to the Beijing government. According to Symantec researchers, the Black Vine has also targeted "organizations from a variety of industries including aerospace healthcare, energy, military defense, finance, agriculture and technology" (Riley and Robertson, 2015, p. 1). This breach was one of the most harmful and led to the resignation of the OPM director Katherine Archuleta. United Airlines restored customers' miles as an apology for the cybercrime attack (Riley and Robertson, 2015).

## COMMUNITY HEALTH SYSTEMS

Community Health Systems is one of the nation's leading operators of general acute care hospitals. The company claims, "the organization's affiliates own, operate, or lease 158 hospitals in 22 states with approximately 27,000 licensed beds. Affiliated hospitals are dedicated to providing quality healthcare for local residents and contribute to the economic development of their communities" (Community Health Systems, 2016). In July 2014, Community Health

Systems confirmed that the computer network was a target of an external cybercriminal attack. The attack could be considered the largest single health data breach by a publicly traded company (Munro, 2014).

On August 18, 2014, Community Healthcare Systems announced its attack of malware exposing patient names, addresses, birthdates, telephone numbers, and social security numbers. This attack was considered a breach under HIPAA. HIPAA is the Health Insurance Portability and Act of 1996, which provides privacy and security provisions for safeguarding medical information. There were 4.5 million patients involved. The perpetrator was labeled as an "Advanced Persistent Threat" which originated in China. The hackers were able to bypass security, successfully copy, and transfer data. Community Health Systems issued a letter of apology with free identity theft protection and a toll free hotline to report any suspicious activity. Community Health Systems increased efforts to better security including surveillance technology, adopting advanced encryption technology, and requiring users to change their passwords (Munro, 2014).

**HOME DEPOT**

Home Depot, the world's largest home improvement retailer, announced its security breach on September 8, 2014. The malware resided in the computer systems from April to September (Smith, 2014). The POS malware attack was identified as a "third party" attack. The company stated that thieves used a vendor's user name and password to enter the perimeter of the network. Home Depot's investigation found that hackers escaped detection by using custom-made malware that had never been seen before. The malware was referred to as "zero days" because it was not spotted by traditional anti-virus software. Credit and debit card numbers and email addresses were stolen. Home Depot warned customers to not open any kind of survey in

return for a reward. There were 2,200 United States and Canada stores affected with 56 million credit or debit cards numbers and email addresses retrieved. Home Depot issued a statement of apology and customers were not responsible for fraudulent charges (Krebs, 2014).

CEO and chairman, Frank Blake, stated, "We apologize for the frustration and anxiety this causes to our customers, and I want to thank them for their patience and support as we work though this issue. We owe it to our customers to alert them that we now have enough evidence to confirm that a breach has indeed occurred. It's important to emphasize that no customers will be responsible for fraudulent charges to their accounts." This cyber attack cost Home Depot $90 million in total. Identity protection services were provided free of charge. The company also announced the future use of the chip and pin technology for better security (Smith, 2014).

**JPMORGAN CHASE & CO.**

JPMorgan Chase is one of the oldest financial institutions in the United States. Currently, they are the leading global financial service firm with assets of $2.4 trillion, operate in more than 100 countries, have over 235,000 employees, and serve corporate, institutional, and government clients. JPMorgan Chase states, "We are a leader in investment banking, financial services, for consumers and small businesses, commercial banking, financial transaction processing and asset management" (JPMorgan Chase & Co., 2016). On October 2, 2014, JPMorgan announced an attack. This attack went unnoticed for over two months over the summer.

The company fell victim to phishing which retrieved a list of applications that run on JPMorgan's computers, names, addresses, phone numbers, and emails of account holders. There were 76 million households and 7 million small businesses affected. The Russians were theorized to be the perpetrators by the FBI. Gery Shalon, Ziv Orenstein, and Joshua Sanuek Aaron were the masterminds behind the attack. Despite their $250 million budget on

cybersecurity, hackers were able to access the servers because the security team had neglected to add a two-factor authentication which is an added layer of protection used by large banks. Fortunately, the information accessed was mainly marketing related rather than banking functions. JPMorgan responded stating that customers were not liable for unauthorized transactions (Tobias, 2014).

**STAPLES**

Staples, a popular office supply store, announced its cybercrime attack October 20, 2014. Staples was a victim of a point-of-sale malware attack which obtained personal information including cardholder names, payment card numbers, expiration dates, and card verification codes (Staples, 2014). It was estimated that 1,400 retail stores across America were impacted affecting 1.6 million payment cards. A group of malware specialists called the "Anunak" were responsible for the attack, this group has made the majority of their profit on attacks on the Russian finance industry (Fox-Brewster, 2014). Staples responded to customers stating that they would offer free identification protection services at no cost including: cost credit monitoring, identity theft insurance, and credit report services (Haselton, 2014).

**SONY CORPORATION**

Sony Corporation, a multinational company specializing in electronics, gaming, and entertainment, announced its cybercrime attack on December 12, 2014. The first attack occurred in October and went unknown. The Monday before Thanksgiving, Sony Pictures employees logged into computers and were greeted with an image of a red skeleton with the words "#Hacked by #GOP" and a threat to release data if a request was not met. The FBI released a memo warning of a destructive type of malware. This malware compromised personal information, social security numbers, salaries, addresses, and contracts. In addition, threats were

made against employees. Documents had been stolen, internal servers were wiped, and approximately 75% of the servers had been destroyed. Five movies including the new release of "Annie" were released (Barnes and Ceiply, 2014).

There were 47,000 employees and actors affected by the attack performed by a group called the "Guardians of Peace." This group was suspected to be part of the North Korean Government. This ultimately cost Sony $35 million in technical repairs. Fingers were pointed at the North Korean government because the movie "The Interview" included the fictional assassination of Korean leader Kim Jong-un. This content was considered a hint towards terrorism and was taken offensively. Sony was urged to stop the "movie of terrorism" because it was invoking the September 11, 2001 terrorist attacks (Peterson, 2014). The movie's release was originally scheduled for Christmas Day, but it was cancelled.

Sony was criticized by the White House. Obama scolded Hollywood studies for caving into what he described as a foreign dictator imposing censorship in America. This was the first time the United States had directly accused another country of a cyberattack of such magnitude. Hacked information was publicized that stated some female stars were paid less than male co-stars, Angelina Jolie was named a "minimally talented spoiled brat," and George Clooney received negative reviews for an early released movie. The FBI found that hackers had used digital techniques to steal the credentials and passwords from a system administrator (Holland and Spetalnick, 2014).

## ANALYSIS AND RESULTS

A t-test was used to determine if the cybercrime had a significant impact on each company's stock price. The change in the stock price was compared with the change in the Dow Jones Industrial Index. The results indicate that after the announcement of cybercrime, there is a

negative, but not significant impact on the market value of the stock prices. Citigroup, Universal Continental Holdings, and Community Health Systems are a prime example of the stock price changing briefly. The price changed the day after the announcement, but then went back up. Target, Anthem, Michaels, Home Depot, and Sony all had decreases in their stock price after the announcement. JPMorgan & Chase Co. and Staples were the only two that after the announcement the stock price did not decline. Table 4 shows the percent change in stock price compared to the Dow Jones Industrial Index.

[See Table 4: Effect of Cybercrime News on Stock Price]

Other factors, such as interest rates, economic outlook, inflation, deflation, economic and political shock and changes in economic policy, could also factor into the changes in the stock prices after the date of the announcement of the cybercrime. A majority of the cybercrime cases were retail store companies or related to the healthcare system. This could be an indicator that retail stores and healthcare systems might be more vulnerable to cybercrime than other types of businesses.

## NEGATIVE EFFECTS OF CYBERCRIME

A history of cybercrime can be detrimental to a company from a marketing, ethical, and internal control point of view. From a marketing standpoint, the company could ultimately lose business if it does not attract shareholders. A company with a history of cybercrime may deter potential shareholders from investing in the company because of its lack of security and stability of their transactions. This vulnerability can lead to the decrease of the market value of the company due to the lists of concerns from financial analysists, investors, and creditors. This will not lead to the overall success of the business.

Ethically, cybercrime is an issue because it is sometimes committed within the company. Companies should be extremely selective when hiring potential employees who work with secured access and confidential information. External of the company, hackers seem to overcome the ethical dilemma of whether or not cybercrime is a morally ethical action. People feel the need to create cybercrime programs to sell on the black market and expose or sell personal information for personal financial gain rather than earning money legally. Damaging a company's reputation and causing turmoil in people's personal lives is a matter of ethics in accordance to what each individual deems acceptable for profit or gain.

Cybercrime is also an issue of internal control for a company. As a successful business, companies need strong internal controls to safeguard their protected information and transactions. Clients trust companies with secure information and for information to be confidential. Companies should have adequate preventive measures to keep customers safe, as they should be a priority of the company. This calls for innovative and stronger technology to alert companies and clients faster when cybercrime is detected.

## CYBERCRIME PREVENTION

Today, there are many forces at work against cybercrime. The FBI now ranks cybercrime as one of its top law enforcement activities (Granville, 2015). The Cyber Division at the FBI Headquarters works "to address cybercrime in a coordinated and cohesive manner" staffed with 56 field offices to "investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud." The FBI also have a partnership with other federal agencies such as the Department of Homeland Security to resolve these matters. The Internet Crime Complaint Center also provides the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspicious activity.

Interpol is another organization that is committed to fight against cybercrime. Interpol mainly focuses on operational and investigative support, cyber intelligence and analysis, digital forensics, innovation and research, capacity building, and National Cyber Reviews (FBI, 2016.).

Security improvements include using Preventive measures to protect personal computers, identity, and safeguard transactions. These measures include:

- Keep firewalls turned on to protect computers from hackers.
- Install or update antivirus software and antispyware technology.
- Keep operating systems up to date.
- Be cautious of downloaded files and false email attachments.

Companies should also create a plan of action to manage cybercrime if it falls under attack. They should have a strategy to manage the publicity, have a statement ready for the media, and contacts for investigation. Companies should also budget money for repairs, reimbursement, and for future protection (FBI, 2016).

## CONCLUSIONS

Cybercrime is a prevalent problem facing publicly traded companies. Cybercrime can cost businesses million in stolen assets or information, reputation, and can disrupt marketing activities and shareholder value. This study examines the types and costs of cybercrime, the threats to cyber security, and analyzes the impact of the announcement of cybercrime on the stock price of ten companies. Results indicate that cybercrime negatively affected stock prices the statistical analysis indicated the effect was not significant.

Cybersecurity is necessary to avoid becoming victim of cybercrime. Information systems should be regularly monitored, background checks should be done for all employees, and warnings of cybercrime should not be ignored. Companies should also create a plan of action for

responding to cybercrime. Preventive measures should be emphasized as they are less costly than the repairs. Companies should invest into the cyber protection of their company.

The current study could be extended by researching additional publicly traded companies that have been victims of cybercrimes. A larger sample size may help better determine the type of industry most susceptible to cybercrime.

**REFERENCES**


Anthem. 2016. “About Anthem, Inc.” Anthem. Retrieved on 2 November 2016 from https://www.antheminc.com/AboutAnthemInc/index.htm.

Barnes, Brooks and Cieply, Michael. 2014. “Sony Cberattack, First a Nuissance, Swiftly Grew Into a Firestorm.” The New York Times. Retrieved on 2 November 2016 from http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.

Community Health Systems. 2016. “Company Overview.” Community Health Systems. Retrieved on 13 November 2016 from http://www.chs.net/#skip-menu.

Dash, Eric and Schwartz, Nelson. 2011. “Thieves Found Citigroup Site an Easy Entry.” The New York Times. Retrieved on 2 November 2016 from http://www.nytimes.com/2011/06/14/technology/14security.html.

Dowell, Andrew. 2014. “Michaels Warns of Possible Data Breach.” The Wall Street Journal. Retrieved on 3 November 2016 from http://www.wsj.com/articles/SB10001424052702303277704579344542352677628.

Granville, Kevin. 2015. “9 Recent Cyberattacks Against Big Businesses.” The New York Times. Retrieved on 2 November 2016 from http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=0.

FBI. 2016. "Cyber Crime." FBI. Retrieved on 2 October 2016 from https://www.fbi.gov/investigate/cyber.

Fox-Brewster, Thomas. 2014. "Meet Anunak - The Hacker Crew That Owned Staples And Earned $18m In 2014." Forbes. 22 Dec. 2014. Retrieved on 2 October 2016 from http://www.forbes.com/sites/thomasbrewster/2014/12/22/anunak-hackers-who-hit-staples/#4789489a3334.

Harris, Elizabeth. 2014/ “Michaels Stores’ Breach Involved 3 Million Customers.” The New York Times. Retrieved on 3 November 2016 from http://www.nytimes.com/2014/04/19/business/michaels-stores-confirms-breach-involving-three-million-customers.html?_r=0.

Haselton, Todd. 2014. “Staples: 1.16 Million Credit Cards Affected in Cyber Attacks.” Retrieved on 15 November 2016 from http://www.technobuffalo.com/2014/12/22/staples-1-16-million-credit-cards-affected-in-cyber-attacks/.

Holland, Steve and Spetalnick, Matt. 2014. “Obama vows U.S. response to North Korea over Sony cyber attack. REUTERS. 19 Dec. 2014. Retrieved on 10 November 2016 from http://www.reuters.com/article/us-sony-cybersecurity-usa-idUSKBN0JX1MH20141219.

INTERPOL. 2016. "Cybercrime." Interpol. Retrieved on 2 October 2016 from http://www.Interpol.int/Crime-areas/Cybercrime/Cybercrime.

ITBusinessEdge. 2016. “Eight Reasons Why Cyber Attacks Hit Retailers.” ITBusinessEdge. Retrieved on 1 November 2016 from http://www.itbusinessedge.com/slideshows/eight-reasons-why-cyber-attacks-hit-retailers-10.html.

JPMorgan Chase & Co. 2016. “About Us.” JPMorgan Chase & Co. Retrieved on 13 November 2016 from https://www.jpmorganchase.com/corporate/About-JPMC/about-us.htm.

Julien, Ted. 2016. “Defining Moments in the History of Cyber-Security and the Rise of Incident Response.” InfoSecuirty. Retrieved on 2 November 2016 from http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/.

Krebs. 2014. “Home Depot: Hackers Stole 53M Email Addresses.” KrebsonSecurity. Retrieved on 13 November 2016 from https://krebsonsecurity.com/2014/11/home-depot-hackers-stole-53m-email-addreses/.

Mathews, Anna Wilde. 2015. "Anthem: Hacked Database Included 78.8 Million People." Wall Street Journal. 24 Feb. 2015. Web. 01 Oct. 2016. Retrieved on 2 October 2016 from http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364.

McAfee. 2016. “Net Losses: Estimating the Global Cost of Cybercrime: Economic Impact of Cybercrime.” McAfee. Retrieved on 2 October 2016 from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

Mercer, Edward. 2016. “Causes of Cybercrime.” Tech in our everyday life. Retrieved on 1 November 2016 from http://techin.oureverydaylife.com/causes-cyber-crime-1846.html.

Morgan, Steve. 2016. "Cyber Crime Costs Projected To Reach $2 Trillion by 2019." Forbes. 17 Jan. 2016. Retrieved on 2 October 2016 from http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#81fe0503bb0c.

Munro, Dan. 2014. “Cyber Attack Nets 4.5 Million Records From Large Hospital System.” Forbes. Retrieved on 3 November 2016 from http://www.forbes.com/sites/danmunro/2014/08/18/cyber-attack-nets-4-5-million-records-from-large-hospital-system/#c8522818bce0.

Norton. 2016. "Cybercrime - The Definition of Cybercrime.” Norton. Retrieved on October 2016 from http://us.norton.com/cybercrime-definition/.

Paganini, Pierluigi. 2015. "Anthem Breach: A Slow and Silent Attack." Wall Street Journal. Retrieved on 1 October 2016 from http://securityaffairs.co/wordpress/33582/cyber-crime/anthem-breach-slow-silent-attack.html.

Peterson, Andrea. 2014. “The Sony Pictures hack, explained.” The Washington Post. Retrieved on 2 November 2016 from https://www.washingtonpost.com/news/the - switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

Rashid, Fahmida. 2014. “How Cybercriminals Attacked Target: Analysis.” Security Week. Retrieved on 3 November 2016 from http://www.securityweek.com/how-cybercriminals-attacked-target-analysis.

ReadyCloud. 2016. “Ecommerce Statistics All Retailers Should Know.” ReadyCloud. Retrieved on 11 November 2016 from https://www.readycloud.com/info/ecommerce-statistics-all-retailers-should-know.

Riley, Michael and Robertson, Jordan. 2015. “China-Tied Hackers That Hit US Said to Breach United Airlines.” Bloomberg. Retrieved on 3 November 2016 from http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines.

Smith, Katherine and Smith, Murphy and Smith, Jacob. 2003. “Case Studies of Cybercrime and its Impact on Marketing Activity and Shareholder Value.” Retrieved on 1 October 2016 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1724815.

Smith, Gerry. 2014. “Home Depot Admits 56 Million Payments After Cyber Attack.” The Huffington Post. Retrieved on 13 November 2016 from http://www.huffingtonpost.com/2014/09/18/home-depot-hack_n_5845378.html.

Staples. 2014. "News Release." Staples. Retrieved on1 October from http://investor.staples.com/phoenix.zhtml?c=96244&p=irol-newsArticle&ID=2001185.

Statista. 2016. “B2B E-Commerce.” Statista. Retrieved on 2 October 2016 from https://www.statista.com/markets/413/topic/458/b2b-e-commerce/.

Statista. 2016. “B2C E-Commerce.” Statista. Retrieved on 2 October 2016. from <https://www.statista.com/markets/413/topic/457/b2c-e-commerce/>.

Tobias, Sharone. 2014. “2014: The Year in Cyberattacks.” Newsweek. Retrieved on 2 November 2016 from http://www.newsweek.com/2014-year-cyber-attacks-295876.

Wavefront. 2016. “A Brief History of Cybercrime.” Wavefront Consulting Group. Retrieved on 11 November 2016 from http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html.

Weise, Elizabeth. 2015. "Massive Breach at Health Care Company Anthem Inc." USA Today. Retrieved on 1 October 2016 from http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/.

**Table 1**

**Timeline of Cybercrime**

| Year | Event |
|---|---|
| 1946 | The first electronic computer was constructed at the University of Pennsylvania. |
| 1970 | The first use of electronic data interchange (EDI) are applied. |
| | A teller at New York's Dime Savings Bank used computer to embezzle over $2 million. |
| | Rootkits are created. |
| 1978 | The first spam email sent over ARPAnet, the US Defense Department network by a Digital Equipment Corporation marketing executive. |
| 1982 | The first virus sent from a high school student, Rich Skrenta, who wrote Elk Cloner for Apple II computers. |
| 1984 | Science fiction author William Gibson coins the term "cyberspace" in his novel, Nueromancer. |
| 1988 | Robert T. Morris, graduate student from Cornell University, created a worm that hooked up to governments' ARPAnet. |
| 1989 | A diskette claiming to contain a database of AIDS information was mailed to thousands of AIDS researchers and subscribers to a UK computer magazine. |
| 1994 | Inception of business to customer (B2c) e-commerce. |
| | Pizza Hut sold pizza on website. |
| | The first cyberbank, First Virtual, opens. |
| 1996 | Phishing was created. |
| 1997 | Internet host computers (i.e., computers with a registered IP address) exceed 200 million. |
| | Users in over 150 countries are connected to Internet. |
| 2000 | Social networking launches (My Space, Facebook, etc.). |
| | Denial of service attacks begin with Canadian hacker MafiaBoy who took Down high-profile websites including Amazon, CNN, and Yahoo. |
| 2003 | SoBig email worm was considered an attempt to create large-scale botnets. |
| 2005 | Albert Gonzalez masterminded criminal ring that stole around 45.7 million payment cards used by customers of US retailers. |
| 2010 | Stuxnet is discovered which targets industrial software and equipment. |
| 2011 | Advanced persistent threat (APT) develops in which a foreign nation state government with capacity and intent to persistently and effectively target a specific entry. |
| 2013 | Target Corporation hackers intercepted 110,000,000 records worth of information. |
| | Anthem cyberattack is considered the largest healthcare breach to date. |
| 2014 | Community Health Systems cyberattack created breach under HIPPA. |

Adapted from: Smith et al. 2010

**Table 2**

**Common Types of Cybercrime**

| Cybercrime | Definition |
|---|---|
| Botnet | A botnet is network of private computers infected with malicious software and controlled as a group without the owner's knowledge, e.g., to send spam messages. |
| Computer Virus | A computer virus is a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data. |
| Cybercrime | Cybercrime is crime conducted via the Internet or some other computer network. |
| Cyberterrorism | Cyberterrorism is the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society. |
| DDoS attack | DDoS is short for Distributed Denial of Service. It is a type of attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system. |
| E-Fraud | E-Fraud is the activity of obtaining money illegally using the Internet. |
| Encryption | Encryption is encoding electronic information in such a way that only parties who have a password can access the information. |
| Identity Theft | Identity theft is the fraudulent acquisition and use of a person's private identifying information, usually for financial gain. |
| Online Credit Fraud | This term is wide-ranging for theft and fraud committed using or involving a payment card and fraudulent source of funds in a transaction. |
| Malware | "Malicious software" that refers to software programs that are designed for destruction or unwanted actions on a computer system. |
| Phishing | Phishing attempts to trick Internet users into divulging their personal information for use or resale by criminals. |
| Ransomware | Ransomware is a type of malicious software designed to block access to a computer system until a sum of money. |
| Rootkit | Rootkit is a software that enables continuous privileged access to a computer white actively hiding its presence from administrators. |
| Software Piracy | Software piracy is the illegal copying, distribution, or use of software. |
| Spam | Spam occurs when the same message is sent indiscriminately to a large number of recipients on the Internet. |
| Virus | A virus is a computer program that that can copy itself, and infect a computer, and spread when its host is taken to the target computer. |
| Worm | A worm is a self-replicating computer program that sends copies of itself to other nodes over a network. |

Adapted from: Smith et al. 2010

**Table 3**

**Companies and Cybercrime**

**Panel A:**

| Company | Ticker Symbol | Type of Crime | Targeted Information |
|---|---|---|---|
| Citigroup Inc. | C | malware | names, account numbers, contact info, SSN, birthdates, DOB, card expiration dates, CVV |
| Target, Corporation | TGT | POS malware | credit/debit cards names, expiration dates, CVV |
| Anthem | ANTM | malware | employment info, income data |
| Michaels | MIK | POS malware | payment card info, card numbers, expiration date |
| United Continental Holdings INC | UAL | Malware | passenger flight and destination info, SSN from OPM |
| Community Health Systems | CYH | malware | patient names, addresses, birthdates, telephone, SSN, considered breach under HIPAA |
| Home Depot | HD | malware | credit/debit card numbers, email addresses |
| JP Morgan Chase & Co. | JPM | phishing | list of applications that run on JPMorgan's computers, names, addresses, phone numbers, emails of account holders |
| Staples | SPLS | Black POS malware | cardholder names, payment card numbers, expiration dates, card verification codes |
| Sony Corporation | SNE | malware | SSN, salaries, addresses, contracts, threats against SPE, employees, threats to distribute movies |

**Panel B:**

| Ticker Symbol | Victims | Perpetrator | Response |
|---|---|---|---|
| C | 360,000 accounts | Lulzsec | reissued with new cards with notification letter, customers not liable for fraud |
| TGT | 70 million accounts | Daniel Dominguez Guardiola and Mary Carmen Vaquera Garcia | one year free credit monitoring and identity theft, resignation of Beth M. Joacob-Senior Technology officer, resignation of Gregg Steinhafel-CEO and Chairman, announced timetable to move chip and pin system |
| ANTM | 78.8 million customers and employees | China | letter of apology, AllClear ID 2 years at no cost, hotline, fraud protection and credit freeze info |
| MIK | 3 million customers | Eastern Europe | letter of apology from CEO, hotline |
| UAL | 10,000 accounts, 80% US victims | China | miles restored, resignation of Katherine Archuleta-OPM director |
| CYH | 4.5 million patients | China "Advanced Persistent Threat" | toll free hotline, statement of apology, customers not liable for fraudulent charges, free identity protection services |
| HD | 2,200 US and Canadian stores, 56 million card numbers, 56 million email addresses | third party | customers not liable for fraudulent charges |
| JPM | 76 million households, 7 million small businesses | Gary Shalon, Ziv Orenstien, Joshua Samuel Aaron | not liable for fraudulent charges |
| SPLS | 1,400 retail stores, 1.6 million payment cards | Anunak | no cost credit monitoring, identity theft insurance, credit reporting |

| | | | |
|---|---|---|---|
| SNE | 47,000 employees and actors | Guardians of Peace<br>North Korean Government | Obama scolded Hollywood |

## Table 4

### Effect of Cybercrime News on Stock Price

| | | Percent Change in Company Stock Price around Event Day | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Company** | **Day** -7 | -3 | -1 | 0 | 1 | 3 | 7 |
| 1 | C | 0.37 | 4.09 | 0.98 | 0 | (1.75) | 1.41 | 4.73 |
| 2 | TGT | 1.31 | 0.04 | 2.48 | 0 | (0.60) | (0.78) | 0.59 |
| 3 | ANTM | 4.20 | 0.50 | (2.57) | 0 | 1.59 | (1.17) | 0.09 |
| 4 | MIK | 5.65 | 5.59 | 0.35 | 0 | 1.05 | (0.40) | (0.12) |
| 5 | UAL | 11.14 | 1.21 | (4.24) | 0 | (1.15) | 1.97 | (0.69) |
| 6 | CYH | (6.14) | (4.36) | (1.26) | 0 | 0.49 | (1.12) | 0.16 |
| 7 | HD | 0.36 | (2.00) | 0.87 | 0 | (2.08) | (1.76) | (1.59) |
| 8 | JPM | 1.63 | 0.50 | 0.95 | 0 | 2.62 | 2.40 | 0.43 |
| 9 | SPLS | (1.54) | (1.30) | (3.09) | 0 | 1.30 | 1.79 | 1.30 |
| 10 | SNE | (0.77) | (0.90) | (0.18) | 0 | (4.56) | (6.18) | (8.26) |
| **Avg % Change Stock Price** | | 1.62 | 0.34 | (0.57) | | (0.31) | (0.38) | (0.33) |
| **Avg % Change DJI Index** | | 0.80 | (0.52) | (0.39) | | 0.03 | 0.46 | 0.31 |
| **Significance (prob>)** | | 0.36 | 0.20 | 0.38 | | 0.34 | 0.10 | 0.19 |