Cyber-Crime Effects and Issues on Company and its Stock Market Prices

Vrunda Chaintanya Rana¹ Kanchi Saurabh Parekh² Varsha Girish Tank³
¹,²UG Student ³Assistant Professor
¹,²,³Department of Computer Engineering
¹,²,³SAL Institute of Technology & Engineering Research, Ahmedabad, Gujarat, India

Abstract— Cybercrime is a ubiquitous and crucial threat to publicly traded companies. Even though people have a basic amount of knowledge about “cyber-crime”, the effects of this kind of crime has a great amount of impact on the people’s lives and society. This type of crime many times result in a loss of billion dollars annually to publicly traded companies in the form of stolen assets and lost business. Further, when a company becomes a victim of cyber criminals, it may cause its customers to worry about the security of their business transactions with the company. If the company remains vulnerable to this kind of attacks than it may result in losing its future business. This thesis examines the effects and issues of cyber-crime on the stock market as well as on the company and the customers of the company.

Key words: Cyber, Crime, Cyber Crime, Stock, Market, Computer Crime, Virtual

I. INTRODUCTION

The evolution and use of the computer and the internet have produced enormous possibilities and advantages for businesses including e-commerce, faster transactions, better communication, and increased marketing and publicity. These benefits have generated opportunities for growth and development for business worldwide. Even though it provides a lot of facilities, it also brings a heavy cost of potential threats to security. Cybercrime is a kind of crime that happens in "cyberspace"[8] Cyber – crime has always been a constant and widespread threat to publically traded companies. These type of publically traded companies often suffer through a great amount of loss not only because of the financial loss but also because of the permanent blemish on company’s reputation created by this kind of act. Cyber-crime not only affects the company and its shares but it also affects the loyal customers and the public shareholders of the company. This type of malicious act often results in loss of confidence of the customers and the shareholders of the company. If the company’s cyber security and internal control are not so trustworthy, then the shareholders will move their investments to other safe and secure public traded companies. This may result in company’s reduced market value. If the public traded companies are perceived to be targets of cyber-crime, these companies can lose business. Their market value may decrease as a result of lost business.

There are many ways in which cyber-crime can occur. Generally, it has three categories.[6]

1) Target cyber-crime: The crime in which computer is the target of the offence.
2) Tool cyber-crime: The crime in which a computer is used as a tool in committing the offence.
3) Computer incidental: The crime in which a computer plays a minor role in committing the offence.

This thesis analyses cyber-crime, its issues and its effects on publically traded companies’ stock market prices. This thesis examines the effects of cyber-crime on publically traded company’s stock market price. This thesis focuses on questions like:

1) How does cyber-crime affect marketing activity?
2) Does the negative news about cyber-crime on a company affect its share market value?
3) How does this impact affect routine consumers?

II. LITERATURE REVIEW

A. Categories of Cyber-Crime [8]

1) Target Cyber-crime:
When the computer is being targeted for an attack, the hacker attack the system by either attacking it externally or breaking it in to it. This type of cyber-crime can be considered as the most “Professional” in the above cyber-crime category. In this attack, the hacker attacks the system and exploits it using programming. This type of attackers generally have a strong background of computer science.

Types of Target Cyber-crime are as follow:

1) Hacking
2) Malware
3) Distributed Denial of Service (DDoS)

2) Tool Cyber-crime:
In tool cyber-crime the main tool used for attacking is the computer. Hence for the tool cyber-crimes, the role of the computer is similar to the role telephone plays in telephone fraud [6].

The type of crimes in which tool cyber-crime is used are as follows:

1) Crimes Against Property
   - Theft
- Fraud
- Extortion

2) Crimes Against Persons
- Physical Harm
- Psychological Harm

3) Computer Incidental:
The role played by the computer is minor, in Computer Incidental. The law students might be more familiar to this type of cyber-crime compare to those who has majored in computer science. So, in Computer Incidental cyber-crime the topics related to computer science are comparatively less.

Challenges faced due to this type of cyber-crime are divided in two categories [6].
- Digital Evidentiary Challenge
- Privacy

In most of the cyber-crime news, the hacker is the main culprit. While in some stories the culprits are the ones who have computer expertise which is relatively less than the expertise of hackers. There are different types of cyber-crimes done by these culprits like cyber-terrorism, Electronic theft, Cyber-Spying, online electronic money fraud, phishing. Table 1[8] represents some well-known companies that were affected by cyber-crime.

<table>
<thead>
<tr>
<th>Companies affected by cyber-crime</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo</td>
<td>February 7, 2000</td>
</tr>
<tr>
<td>Amazon</td>
<td>February 8, 2000</td>
</tr>
<tr>
<td>Buy.com</td>
<td>February 8, 2000</td>
</tr>
<tr>
<td>CNN</td>
<td>February 8, 2000</td>
</tr>
<tr>
<td>eBay</td>
<td>February 8, 2000</td>
</tr>
<tr>
<td>E*Trade</td>
<td>February 9, 2000</td>
</tr>
<tr>
<td>ZDNet</td>
<td>February 9, 2000</td>
</tr>
<tr>
<td>Muniowa</td>
<td>March, 2009</td>
</tr>
<tr>
<td>Visa</td>
<td>December, 2010</td>
</tr>
<tr>
<td>MasterCard</td>
<td>December, 2010</td>
</tr>
<tr>
<td>Paypal</td>
<td>December, 2010</td>
</tr>
<tr>
<td>Wordpress</td>
<td>March 4, 2011</td>
</tr>
</tbody>
</table>

Table 1: Cyber-Crime in 2000, 2009, 2010 and 2011

The stock prices of the publically traded company are dependent on the reputation of the company. The stock price of these publically traded companies deter due to blemish on the reputation of the company because of the news stories of cyber-attack on the company. Damages in companies due to cyber-crime varies according to the intensity of cyber-attack. Some cyber-attacks result in closure of the company website while some may result in stealing the confidential data and information. Marketing, ethical and internal control point of view are used to determine the history of cybercrime of a company. From a marketing standpoint, the company may suffer a heavy loss due to cyber-crime, as it would lose the confidence of its shareholders. A company which has been affected by cyber-crime may prevent its potential shareholders from investing in the company due to deficit security and instability of shareholder’s transactions. The vulnerability of the company towards cyber-crime will decrease the market value and reputation of the company as the financial analysts, investor and creditors will be least concerned. This will lead to overall loss of the business. From the ethical standpoint, cyber-crime is a concern because it is many times committed by the employees of the company itself. Companies should be cautious while selecting the employees for the company who will be given a job of high responsibility like secured access and confidential data information. From the perspective of internal control, the company would lose its business and reputation, if it does not have an adequate amount of security for its clients’ confidential information. Cyber-crime not only damages the company reputation but it also damages trade competitiveness, innovation and global economy growth.

The publically traded companies are highly affected by the above damages due to cyber-crime because the effect of the damage caused due to cyber-crime will not only affect the clients and customers, but will also affect company’s shareholders financially as the stock market price of the publically traded company’s stocks will fluctuate due to the news of cyber-attack on that company. This will result in financial loss to shareholders and will also decrease the truth of the shareholders towards the company.

4) Cyber-crime effects on Sony Corporation [9]:
Sony Corporation is a multinational company which is specialized in electronics, gaming, and entertainment. Sony Corporation announced its cyber-crime attack on 12th December 2014. It faced its first attack on October but the attack remained unknown. When the employees of the Sony Pictures logged in to their computers on the Monday before Thanksgiving, they were greeted with the image of a red skeleton with the words “#Hacked by #GOP” and the hackers threatened the company to release the data if the request was not met. A memo warning of a destructive type of malware was released by the FBI. This malware contained personal information, social security number, salaries, addresses, and contacts. They had also made some threats against employees. The damage due to cyber-crime resulted in stolen documents, wiped internal servers, and destruction of approximately 75% of the servers. Five movies were leaked and released.
Sony was criticized by the White House. Hollywood studios was scolded by Obama for caving into what he mentioned as a foreign dictator imposing censorship in the United States of America. On this cyber-attack America, directly accused another country for the first time. The hacked information that was publicized included that some male stars were paid more than their female co-stars. According to FBI, the sensitive information like credentials and passwords were stolen a system administrator by using digital techniques.

On the announcement of the cyber-attack news on Sony Corporation, the stock prices of the company began to fluctuate. The shareholders of the Sony Corporation’s share were bit worried. Even the clients and the investors of Sony Corporation were tensed because of their confidential information like personal data, address, contact information were leaked.

This graph[10] shows the breakdown of the Sony corporation share’s price after the cyber-attack on the company.

![Graph showing Sony Corporation stock price](image)

Fig. 1: Sony Corporation stock price

Thus, this cyber-attack on Sony Corporation affected its reputation which in turn resulted in fluctuation in stock market prices for a short-term.

5) Cyber-crime effects on Amazon, Yahoo and EBay[5]:
A group of cyber-terrorists attacked on internet sites like Amazon.com, Yahoo.com and Ebay.com in February 2000. Hackers made some changes in the program coding. This cyber-attack resulted as chaos in these companies. The problems due to this cyber-attack were very high. The companies suffered a lot during this period. The impact of this attack was so severe that it forced the companies to remain shut for some to repair the damages and recover from the attack. The hackers stole some user’s sensitive data in this attack. After the recovery, changes were made in the company program which helped to prevent future break ‘ins. The security was strengthened for the users.

III. CONCLUSION

The publically traded company is facing a prevalent problem of cyber-crime. Cyber-crime costs business billion in stolen assets or sensitive information, the reputation of the company and can also disrupt marketing activity and shareholders’ value.

We have studied the costs and types of cyber-crime and examined the impact of the announcement of cyber-crime on the price of the stock of Sony Corporation. Cyber-crime slows the speed of innovation by decreasing the rate of return to investors and innovators. We found that cyber-crime negatively affects the stock prices of publically traded companies. Publically traded companies should take necessary steps towards cyber security to protect itself from cyber-crime. A regular monitoring of the information systems should be done and other activities like background check of the employees should be done. And if any warnings related to the cyber-crime is noticed then it should not be ignored. Companies should put more emphasis on preventive measures as these preventive methods are less costly compare to the repairs.

REFERENCES


[9] Amie Jones. Cybercrime Effects on Stock Prices,
