CASE STUDIES OF CYBERCRIME AND ITS IMPACT ON MARKETING ACTIVITY AND SHAREHOLDER VALUE

ABSTRACT:

Cybercrime, also called e-crime, costs publicly traded companies billions of dollars annually in stolen assets and lost business. Cybercrime can totally disrupt a company's marketing activities. Further, when a company falls prey to cyber criminals, this may cause customers to worry about the security of their business transactions with the company. As a result, a company can lose future business if it is perceived to be vulnerable to cybercrime. Such vulnerability can lead to a decrease in the market value of the company, due to legitimate concerns of financial analysts, investors, and creditors. This study examines 10 case studies of publicly traded companies affected by cybercrime, and its impact on marketing activity and shareholder value. The study also describes some of the major types of cybercrime. Results indicate that costs of cybercrime go beyond stolen assets, lost business, and company reputation; cybercrime has a significant negative effect on shareholder value.

INTRODUCTION:

E-commerce is a fundamental part of marketing activity. Most e-commerce takes place on the websites of publicly traded companies. The term „cyberspace" refers to the electronic medium of computer networks, principally the Web, in which online communication takes place. A challenge facing e-business or cyber-business is that it is vulnerable to e-crime, also called cybercrime. Cybercrime can totally disrupt a company marketing activities. Cybercrime costs publicly traded companies billions of dollars annually in stolen assets, lost business, and damaged reputations. Cybercrime costs the US economy over $100 billion per year (Kratchman et al. 2008, Mello 2007). Cash can be stolen, literally with the push of a button. If a company website goes down, customers will take their business elsewhere. In addition to the direct losses associated with cybercrime, a company that falls prey to cyber criminals may lose the confidence of customers who worry about the security of their business transactions. As a result, a company can lose future business if it is perceived to be vulnerable to cybercrime. Such vulnerability may even lead to a decrease in the market value of the company, due to legitimate concerns of financial analysts, investors, and creditors. This study examines types of cybercrime and how they affect marketing activity. In addition, the study reviews 10 case studies of publicly traded companies affected by cybercrime, and its impact on shareholder value. The research questions addressed by this study include:

(1) What are some ways that cybercrime affects marketing activity?

(2) Do cybercrime news stories negatively affect shareholder value? Results suggest that there are a number of types of cybercrime that have detrimental effects on marketing activity. Furthermore, the costs of cybercrime go beyond stolen assets, lost business, and company reputation, but also include a negative impact on the company stock price.

E-BUSINESS AND E-RISK :

Corporate managers must consider e-risks, that is, potential problems associated with ebusiness. Precautions must be taken against e-fraud, malicious hackers, computer viruses, and other cybercrimes. To some extent, electronic business (e-business) began with the early computers in the 1950s. However, not

until development of the World Wide Web in the 1990s did e-business really take off. E-business is exchanging goods or services using an electronic infrastructure. Only a short time ago, using the Internet as a primary way to do business was considered too risky.

Today, e-business is simply business; it's the way business is done in the twenty-first century. The Internet is widely used for both business-to-business (B2B) transactions and business-to-consumer (B2C) transactions. The B2B market is from five to seven times larger than B2C. The B2B market is predicted to exceed $5 trillion in the early 21st century. The B2C market is growing as fast but is characterized by a much smaller average transaction size (Kratchman et al. 2008). In a span of about 50 years, computers transformed the way people work, play, and communicate. The first electronic computer was built in 1946. The computer network that would evolve into the Internet was established in 1969. By the mid-1990‟s, millions of people were using their personal computers to "surf the web."

A brief history of the Web and e-commerce is

E-risk is the potential for financial and technological problems resulting from doing business on the Web (e-business). Changes in economic, industrial, and regulatory conditions mean new challenges. Troublemakers in cyberspace seek systems to infiltrate and misuse. Just for the fun of it, there are some people who try to hack into a business firm‟s computer system. Once access to the system is achieved, intruders can potentially cause major problems by deleting or changing data. Poorly developed accounting systems threaten a company‟s survivability and profitability of e-business operations. Risks related to e-business on the Web include the following (Smith et al. 2003): The changing e-business environment alters risks, so old solutions may no longer work. International business activity expands the scale and scope of risks. Computing 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.

TYPES AND COSTS OF CYBERCRIME:

Cybercrimes are the modern-day counterparts of age-old crime. Before the electronic age, con artists went door-to-door and used verbal communication to gain the confidence of their victims. The modern con artist uses the Internet and online communications to commit crimes. Exhibit 2 lists some of the common types of cybercrime.

CASE STUDIES OF CYBERCRIME:

The following cases were obtained by conducting a search of news stories regarding e-crime, cybercrime, and computer fraud on the Pro-Quest online database of current periodicals 5 and newspapers. The Pro-Quest Research Library provides online access to a wide range of academic subjects. The Pro-Quest database includes over 4,070 tiles, nearly 2,800 in full text, from 1971 forward (Pro-Quest 2010). These cases examined in this study were used because they were listed at the top of the search, involved publicly traded companies, and included full news stories. In February 2000, Amazon.com, Ebay.com, and Yahoo.com were among many Internet sites affected by a group of cyber-terrorists who hacked into the company websites and made alterations to program coding. The problem was so severe that the companies were forced to shut down in order to repair the damage and stop the unauthorized activity. As a result of the site closing, program changes were made to help prevent future break-ins (Kranhold 2000). The Western Union branch of First Data Corp came under attack by a private hacker. In September 2000, the perpetrator hacked into the company site and stole credit-card information for 15,700 customers.

IMPACT OF CYBERCRIME ON COMPANY STOCK MARKET PERFORMANCE:

In many cybercrime news stories, the perpetrator is a hacker. In other stories, the perpetrator has relatively little computer expertise. Types of crime included cyber-terrorism, etheft, netspionage, online credit card fraud, and phishing. Affected companies include dot-com giants Yahoo, Amazon, and EBay, and banks such as JP Morgan Chase and Washington Mutual. Damages vary from the closure of websites to stolen confidential information.

ADDITIONAL THREATS TO COMPUTER SECURITY :

Based on movies and television shows, many people think that the greatest threat to computer security is intentional sabotage or unauthorized access to data or equipment. While sabotage and unauthorized access are serious problems, they are not the main threat to computer security. There are five basic threats to computer security:

1) natural disasters,

2) dishonest employees,

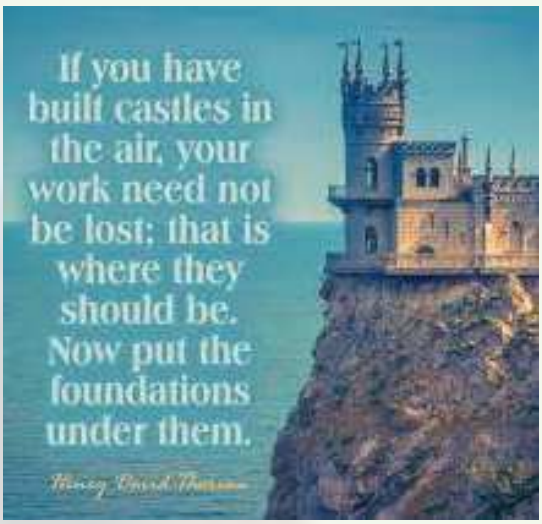
3) disgruntled employees,

4) persons external to the organization

5) unintentional errors and omissions.

CONCLUSIONS:

This study identifies types and costs of cybercrimes, how they interrupt marketing and business activity, and specific cases in which publicly traded companies are affected by cybercrime. In addition, the study analyzes the impact of the cybercrime news stories on shareholder value. Results suggest that costs of cybercrime go beyond stolen assets, lost business, and company reputation, but also include a negative impact on the company‟s stock price. Consequently, publicly traded companies must do all that they can to avoid becoming a victim of cybercrime and its negative impact on marketing activity and shareholder value. To defend against cybercrime, intrusion detection techniques should be established. Techniques include tripwires, configuration-checking tools, and anomaly detection systems. Since prevention techniques are fallible, business firms should also establish procedures for investigation of and recovery from cybercrimes after they occur.



(TE EXTC Student)
Sunil Sahani