AN APPLICATION OF SITUATIONAL CRISIS COMMUNICATION THEORY

CASE STUDY OF TJX- LEAK OF CUSTOMERS' INFORMATION

A RESEARCH PAPER

SUBMITTED TO THE GRADUATE SCHOOL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE

MASTERS OF ARTS

DEPARTMENT OF JOURNALISM

BY

YUNG-YEE LAI

ADVISOR – DR. DUSTIN W. SUPA

BALL STATE UNIVERSITY

MUNCIE, INDIANA

JULY 2010

TABLE OF CONTENTS

Page

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Public relations has been practiced, in its current state, for more than 50 years in the United States, thus allowing researchers to develop multiple theories and practical applications for practice. Crisis management and crisis communication, two areas where much time has been devoted, have received significant attention as crisis is inevitable for business. Distinguished by the eruption of a crisis, crisis management can be divided into two sections, which are the pre-crisis stage and the post-crisis stage. Image repair theory, an important section of crisis management, claims that companies have to handle any crisis appropriately since reputation and credibility are valuable integral assets for any company. In fact, reputation building and maintenance are two key tenants of public relations, and are especially important for a company coming out of a crisis situation.

Situational crisis communication theory (SCCT) is another theory that addresses crisis communication. It is premised on matching the crisis response to the level of crisis responsibility attributed to a crisis. Based on SCCT, crisis managers have to analyze a given situation first so that they can select crisis response strategies which best match the crisis situation. As opposed to the image theory, SCCT focuses on the

situation and environment, and also the reasons the crisis initially occurred. Coombs (1999) states that image repair theory provides a few strategies; however, crisis communication is not solely about strategic ways of dealing with a crisis that has already occurred (p.338). He indicates that situational crisis communication is able to articulate the variables, assumptions and relationships in selecting crisis response strategies to protect an organization's reputation, which ultimately is the goal of an organization in crisis.

The TJX breach of information crisis occurred on January 17, 2007. More than 45.6 million credit card and debit card numbers were stolen. Not only were customers affected, but also all major card brands accepted by TJX. The goal of this research paper is to examine how situational crisis communication theory works effectively in solving problems for TJX case. It is the hope of the researcher that this study serves as a good example for other companies that use on-line database technology as a way to save customers' information in the event of a security breach. As organizations continue to move their business and financial information online, there is an increased need for securing this information, to protect both the organization and the consumer. The key question of the research is "How is situational crisis communication theory used in dealing with the information technology crisis as TJX?"

This case study of the TJX information breach utilizes a content analysis of major news articles surrounding the crisis, to determine how SCCT can be applied to the crisis, specifically, this study examines the communication tools used by TJX in its handling of the crisis. Through this exploration, this study looks to provide the public

relations practitioners a more complete understanding of the situational crisis communication theory as a guide to deal with reputation damages or crises in Information Technology industry in the future.

CHAPTER 2

CASE HISTORY

Background

The TJX companies, Inc. have one of the most flexible business models in the world and great financial strength. The company was founded in 1956 and is based in Framingham, Massachusetts. The crisis happened on January 17, 2007, when TJX announced that someone had illegally accessed one of its payment systems and stolen card data belonging to customers in the U.S., Canada, Puerto Rico and potentially the U.K. and Ireland. All major card brands accepted by TJX were affected, including Visa, MasterCard, American Express and Discover. More than 45.6 million credit card and debit card numbers were stolen from its electronic system over a period of more than 18 months by an unknown number of intruders. It became the largest breach of electronic data in history, affecting customers of its T. J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. and other countries. As a result of that incident, banks and credit unions, including Bank of America Corp., Wells Fargo Bank and Washington Mutual Bank, were forced to cancel and reissue tens of thousands of cards.

Company Background

TJX is one of the largest international apparel and home furniture off-price department stores. According to TJX's website, the company evolved from the Zayre discount department store chain, founded in 1956, which opened its first branch of T.J. Maxx in 1976 and BJ's Wholesale Club in 1984 (NNDB Mapper). In 1988, Zayre decided to sell their name to Ames, a competitor, and renamed itself The TJX Companies, Incorporated. In 1990, TJX entered the Canadian market by owning the five-store Winners chain, and it was not only expanding into an additional store brand division but also went international successfully. According to the international business ranking, TJX Companies, Inc. is a leading company among the retail businesses. It operates 826 T.J. Maxx, 271 HomeGoods, 751 Marshalls, 162 A.J. Wright and The Maxx in United States. It also operates 184 Winners, 68 HomeSense stores, StyleSense in Canada and 212 T.K. Maxx in Europe. In 2004, the company reached 141 in the Fortune 500 rankings, with almost $15 billion in revenue.

TJX is still the leading off-price retailer of apparel and home fashions in the United States and worldwide, with $19 billion in revenues in 2009 (Yahoo finance, 2009) and increased gross profit. An evaluation of the financial data of the TJX companies has shown that there has been little financial impact from the information breach, but as stated earlier, reputation and credibility ultimately have a major impact on a company.

Eruption of the Crisis and the Crisis Management

On January 17, 2007, TJX announced that someone had illegally accessed one of its payment systems and stolen card data belonging to customers in the U.S., Canada, Puerto Rico and potentially the U.K. and Ireland. This was the first time TJX reported that a computer systems intrusion may have compromised the personal data of an undetermined number of its customers. The hackers who had intruded into the systems obtained individuals' credit card, debit card and check information, along with data related to merchandise return transactions (Computerworld Security newsletter, March 21, 2007).

"While TJX has specifically identified some customer information that has been stolen from its systems, the full extent of the theft and affected customers is not yet known," the company said in its statement (January 17, 2007). At first, TJX Companies Inc. was refusing to reveal the size and scope of its data breach and how many customers were affected by the incident. TJX did confirm, however, that a majority of the data involved in the breach belonged to the customers who shopped at stores in the U.S., Canada and Puerto Rico during 2003, and between May and December 2006 (TJX newsletter, January 17, 2007). After TJX released a newsletter about the breach, many media outlets began to report about the incident.

In its January 17 newsletter, TJX stated that the following information was learned through its investigation: 1. An unauthorized intruder accessed TJX's computer systems that process and store information related to customer transactions for its T.J.

Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. and Puerto Rico and its Winners and HomeSense stores in Canada; 2. TJX was concerned that the intrusion might extend to the computer systems that process and store information related to customer transactions for T.K. Maxx in the U.K. and Ireland; 3. The portions of the information stored in the affected part of TJX's network regarding credit and debit card sales transactions in TJX's stores (excluding Bob's Stores) in the U.S., Canada, and Puerto Rico during 2003, as well as the period from mid-May through December, 2006 might have been accessed on this intrusion. Also, TJX had provided the credit card companies and issuing banks with information on these and other transactions; 4. TJX was in the process of carrying out investigations to determine whether additional customer information may have been compromised; 5. TJX had identified a limited number of credit card and debit card holders whose information was removed from its system and had provided this information to the credit card companies; 6. TJX tried to identify a relatively small number of customer names with related drivers' license numbers that were also removed from its system, and contact these individuals directly after breach happened. TJX only indicated that "a relatively small number" of customers' driver's license information was stolen from the compromised systems. Specific numbers were not released by TJX at this time, causing many customers to question whether their information had been compromised.

TJX hired IBM and General Dynamics Corp. to monitor and evaluate the intrusion, and to help the company identify the extent of the data compromise. These two companies helped TJX shore up its security following the breach, and assisted TJX

in further securing its computer systems and implementing security upgrades. TJX stated it was conducting a full investigation of the intrusion with the assistance of several leading computer security and incident response firms and was seeking to determine what customer information may have been compromised (IT World Canada, January 21, 2007). TJX also notified the U.S. Department of Justice and Secret Service, and the Royal Canadian Mounted Police of the data breach, and provided all assistance requested by the law enforcement agencies in an attempt to help track down the perpetrators.

While waiting for the results of investigation, TJX formed a crisis management team to deal with the crisis. In an attempt to protect and repair the company's damaged reputation, Chairman and Acting Chief Executive Officer of The TJX Companies, Inc., Ben Cammarata offered an apology to its customers, "We are deeply concerned about this event and the difficulties it may cause our customers. Since discovering this crime, we have been working diligently to further protect our customers and strengthen the security of our computer systems and we believe customers should feel safe shopping in our stores (TJX newsletter, January 21, 2007)." Following the statement, TJX set up toll-free numbers for customers in the United States, Canada and the United Kingdom who wanted to express concerns over the breach of information. In addition, TJX committed to providing its customers with more information as it became available and indicated that the strength of its computer system's security was improved significantly. The TJX website was used as a primary communication tool to both affected consumers and the media, and included a statement for consumers to carefully review their account

statements and immediately notify their credit or debit card company or bank if they suspect fraudulent use. It also reminded all customers to be wary of potential scams as a result of the data breach, and urged them not to provide any personal information about their bank accounts to anyone who might contact them by phone or e-mail.

Meanwhile, TJX notified and began working closely with the major credit card companies (American Express, Discover, MasterCard and VISA) and entities that process customer transactions. According to Computerworld Security newsletter (January 17, 2007), an e-mail from Visa's vice president stated, "Visa is working with law enforcement officials and TJX to investigate the compromise." MasterCard responded that, "TJX has instructed the banks that issued the cards to monitor accounts for suspicious activity, and MasterCard will continue to both monitor this event and take steps to safeguard account information (Computerworld Security newsletter, January 17, 2007)." The credit card companies, however, also indicated that organizations need to take steps to protect consumer information.

On February 21, 2007, to relieve the public's concerns and questions, TJX posted announcements on its website (www.tjx.com), giving updates of the latest information regarding the computer systems intrusion. Carol Meyrowitz, the new President and Chief Executive Officer of The TJX Companies made an apology first: "Let me begin by telling our customers personally how much I regret any problems or inconvenience they may have experienced as a result of the unauthorized intrusion into our computer system. Our investigation is ongoing, and we are providing an update today on new developments (TJX newsletter, February 21, 2007)." TJX also announced that they had

hired 50 computer security experts to work on the investigation and to strengthen the security of its computer systems. The results of the investigation indicated that the affected systems were based in Framingham, Boston at the company headquarters, where information related to payment cards, checks and merchandise returned without receipts was processed and stored (ComputerWorld, March 29, 2007). The fallout from the breach had been widespread, with banks and credit unions in the United States and in Canada being forced to block and reissue thousands of cards. Furthermore, TJX had previously believed that the intrusion had taken place only from May 2006 to January 2007. Investigations however revealed that their computer systems had been hacked as from July 2005 and on various subsequent dates in the same year. There was, however, no compromise of customer data after mid-December 2006. Information from at least 45.6 million credit cards had been stolen by unknown intruders who had managed to gain access into the company's computer transaction processing systems between July 2005 and mid-January 2007. Investigators had arrived at the 45.6 million figure by extracting data from records of transactions processed between December 31, 2002 and November 23, 2003.

On March 14, 2007, U.S. Federal Trade Commission (FTC) launched an investigation into the TJX Companies. One week later, law enforcement officials in Florida arrested six individuals suspected of carrying out a fraud scheme built around the misuse of credit card data stolen from TJX on March 21, 2007 (ComputerWorld, March 21, 2007). From news reports, the suspects had bought large quantities of Wal-Mart gift cards with the stolen credit card accounts, and kept redeeming the cards in different

locations. According to Florida officials, the losses experienced by Wal-Mart and the banks issuing the credit cards were more than $8 million.

After the suspects were arrested, TJX concentrated its efforts on dealing with compensation issues with banks and credit card companies. Several lawsuits were filed against TJX after the breach was announced. According to TJX's annual report in March, there were 12 lawsuits against the company in the U.S. and six more in Canada. A group of Massachusetts banks had filed a lawsuit for the cost of replacing consumers' credit cards and other damages, and the Arkansas Carpenters Pension Fund, one of TJX's shareholders, had commenced proceedings to open up the company's books. In addition to the litigation, the U.S. Federal Trade Commission and a group of 30 states' Attorneys General started separate investigations. The Office of the Privacy Commissioner of Canada also initiated a formal investigation.

On April 24, 2007, Massachusetts Bankers Association (MBA) also announced that a Boston Court had filed a law suit against TJX for security breach. MBA required TJX to compensate $118 million dollars to cover costs and potential liability. This suit included $11 million in security consultancy fees and other expenses directly related to the attack and a contingency fund of $107 million to cover liability payments arising from pending lawsuits. Many banks from different states joined this suit and become plaintiffs (iTHome news, April 26, 2007). Plaintiffs in this case included the Connecticut Bankers Association, the Main Association of Community Banks, and an association representing almost 300 Northeastern banks in the US.

Interestingly, TJX's sales were not affected by its legal problems. On August 14, 2007, TJX announced its profits and its earnings had increased 9% to $4.3 billion for the second quarter ended by July 28, 2007. Consolidated comparable store sales also increased 5% over 2006. It seemed that the security breach crisis had not influenced the selling volume for TJX. Results from a survey taken in England however indicated that the majority UK consumers (1200) would take their business elsewhere in the event of loss of customer data as a result of a security breach or hack attack (The Register news, April 17, 2007). Carol Meyrowitz, President, TJX's CEO stated , "We have continued to learn more about the computer intrusion(s) and are now able to estimate the Company's liability. Over the past months, we have worked diligently to further strengthen the security of our computer systems. Our customers remain our top priority, and I sincerely thank them for their support during this time (TJX newsletter, August 14, 2007)."

Eight months after crisis, the leader of an identity theft ring that stole credit card numbers from TJX was sentenced to five years in prison and fined US$600,000 dollars (PC World, September 15, 2007). On September 24, 2007, TJX offered settlements to the affected customers. The company provided three years of credit-monitoring services along with identity theft insurance coverage for all consumers whose driver's licenses or other personal data had been compromised by the massive data breach (PC World, September 24, 2007). The settlement offer included: 1. Reimbursement to consumers who had to replace their driver's licenses because of the compromise; 2. Shopping vouchers redeemable in TJX stores in the U.S, Canada and Puerto Rico for customers who had to change bank and credit card information because of the breach; 3. A one-

time, three-day customer appreciation event at which it all goods were offered at a 15 percent discount. TJX CEO Carol Meyrowitz said in a statement, "This proposed settlement, which covers all class actions in the U.S., Canada and Puerto Rico, addresses the different ways customers have told us they have been impacted by the intrusion(s), importantly; we truly appreciate our customers' continued patronage. TJX has been working diligently to reach a settlement that offers a good resolution for our customers (TJX newsletter, September 24, 2007)."

On November 30, 2007, TJX announced that it had reached a settlement agreement with Visa U.S.A. Inc. and Visa Inc. TJX agreed to fund up to a maximum of $40.9 million in alternative recovery payments. The agreement also contained a number of other provisions including Visa's suspension and rescission of specified fines. "Based on everything we have done, I believe customers should feel safe shopping in our stores. We value our customers' trust and I want our customers to know that I am deeply committed to continuing to address the security of our computer systems, and that TJX will provide periodic updates as we learn more, said by Carol Meyrowitz (TJX newsletter, February 21, 2007)."

Another announcement with a settlement agreement with the Bankers Association was released on December 18, 2007. TJX entered into settlement agreements with all but one of the seven banks and bankers associations that had sued TJX in a punitive class action as a result of the intrusion(s) into TJX's computer system. Under the agreements, the Massachusetts Bankers Association, Connecticut Bankers Association and Maine Association of Community Banks, along with Eagle Bank, Saugusbank, and Collinsville

Savings Society, would dismiss all of their claims against TJX. Carol Meyrowitz stated that "The TJX experience underscores broader challenges facing the U.S. payment card system that require urgent action by merchants, banks, payment card companies and associations, and we look forward to greater cooperation in order to better serve and protect customers" (TJX newsletter, December 18, 2007). The following year, TJX updated the settlement agreement with MasterCard. TJX had agreed to pay up to $25 million in the form of alternative recovery payments. The announced settlement with MasterCard International Incorporated and its issuers was completed on May 14, 2008.

In 2009, two years after the crisis occurred, TJX tried to close the book on this infamous security breach. TJX fulfilled the promise it made on September, 2007, and held an appreciation event for its customers. As promised, it rewarded customers with a special sale, offering 15 percent discounts in all its US and Canadian stores on January 22, 2009. This one-day "Customer Appreciation" sale was billed as the firm's way of expressing its appreciation for customers for retaining their loyalty after the information breach (The Register, January 23, 2009). All the customers across the US and Canada were offered a 15 percent discount for one day only at any of the TJX outlets, including TJ Maxx, HomeGoods and Marshalls stores. The sale was originally suggested as part of a court settlement with banks over the consequences of the breach; however, the stipulation failed to make it into the final court agreement. TJX however, still decided to hold this event for its customers.

In June, 2009, the last chapter of this information leak crisis was the settlement with a group of attorney generals regarding the 2005 and 2006 Cyber Intrusion(s) from

TJX. On June, 23, TJX announced that it had settled with a multi-state group of 41 attorney generals, resolving the states' investigations relating to the criminal intrusion(s) into TJX's computer system. Jeffrey Naylor, Chief Financial and Administrative Officer of The TJX Companies, Inc., stated that "This settlement furthers our goal of enhancing consumer protection, which has been central to TJX (TJX newsletter, June 23, 2009). Under this settlement, TJX and the attorney generals had agreed to take leadership roles in exploring new technologies and approaches to solving the systemic problems in the U.S. payment card industry. Mr. Naylor also said, "This settlement furthers TJX's efforts to unite retailers, law enforcement, banks, and payment card companies to consider installing in the U.S. the proven card security measures that are already in use throughout much of the world (TJX newsletter, June 23, 2009)." Under the settlement with the attorneys, TJX agreed to: 1. Provide $2.5 million to establish a new Data Security Fund for use by the States to advance effective data security and technology; 2. Provide a settlement amount of $5.5 million together with $1.75 million to cover expenses related to the states' investigations; 3. Certify that TJX's computer system meets detailed data security requirements specified by the States; and 4. Encourage the development of new technologies to address systemic vulnerabilities in the United States payment card system.

In conclusion, TJX confirmed that its systems were first accessed illegally in July 2005 and then several times later in 2005, 2006 and even once in the January 2007. The company had spent about $5 million in connection with the breach. Several lawsuits had been filed against it since the data breach was announced. By December 2007, 11 people had been charged with a variety of ID fraud and hacking offences over the breach, some

of whom had already pled guilty as part of various plea bargaining arrangements (The register news, January 23, 2009). TJX closed the case by setting agreements with banks and paying $97.5 million for covering the costs and potential liability. TJX also established an information security fund and paid an investigation fee for each state in the U.S.A. It is estimated this breach cost TJX $1 billion in the five years following the breach in costs for consultants, security upgrades, attorney fees and damage-control marketing. Based on the case history and information collected from media sources in U.S., Canada, Europe and Asia, this study will review TJX breach crisis and discuss how situational crisis communication theory was used by TJX to deal with the crisis.

CHAPTER 3

LITERATURE REVIEW

Crisis Management

"A crisis can be defined as an event that is an unpredictable, major threat that can have a negative effect on the organization, industry, or shareholders if handled improperly" (Barton, 1993, p. 2). Organizations may face serious challenges anytime, so crisis management is one of the most important public relations functions for organizations. The Oxford Dictionary describes a crisis as "a time of intense difficulty or danger." As Dilenschneider (2000) noted in *The Corporate Communications Bible*, all crises threaten to tarnish an organization's reputation (p. 46). Contrary to popular brief, a crisis may not be necessarily bad. It is merely characterized by a certain degree of risk and uncertainty (Fink, 1986, p. 84). Undeniably, a well-managed crisis can help an organization to overcome a predicament and lead it into a better condition; however, a poorly-managed crisis can result in serious harm to stakeholders, losses for an organization or end its very existence.

Crisis management is a process designed to prevent or lessen the damage a crisis can inflict on an organization and its stakeholders. It is also the art of removing much of

the risk in uncertainty, thereby allowing those concerned to achieve more control over the destiny of an organization, and thus creatively exercising the role of management leadership (Darling, Shelton and Walker, 2002, p. 48).

Based on the progress of crises, a crisis can be divided into three stages, which are (1) pre-crisis phase, (2) crisis response phase, and (3) post-crisis phase. The pre-crisis phase focuses on prevention and preparation. The crisis response phase deals with the crisis and how to rebuild an organization's or individual's damaged reputation. The post-crisis phase prepares for the next crisis and fulfills commitments made during the crisis phase including the provision of follow-up information. Both Barton (2001) and Coombs (2006) document that organizations are better able to handle crises when they (1) have a crisis management plan (CMP) that is updated at least annually, (2) have a designated crisis management team, (3) conduct exercises to test the plans and teams at least annually, and (4) pre-draft some crisis messages.

In the pre-crisis phase, communication with the stakeholders is of utmost importance. Dissemination of information through the news media allows an organization to fast reach a wide array of publics. Lerbinger (1997) and Fearn-Banks (2001) devote considerable attention to media relations in a crisis. They both suggest that a media spokesperson should be trained beforehand if they are to handle a crisis effectively. Other than the news media, websites and intranet sites can also help an organization to provide quick response and reach the public. Taylor and Kent's (2007) study finds that having a crisis website is a best practice for using the Internet during a crisis (p. 140).

Crisis managers should utilize some form of a web-based response or risk appearing ineffective. This supports Coombs (2007), who is of the view that the crisis manager should work on a unique website, the intranet, and a mass notification system. Having a crisis website is the best practice for using the Internet during a crisis as it plays an important function for the organization as the formal source to present the crisis information.

Once a crisis has happened, the stakeholders, including the news media, will turn to the Internet to get information about it (Corporate Leadership Council, 2003). An intranet site also provides a direct approach that usually allows only employees, suppliers, and customers to access the relevant information. A mass notification system includes the contact information of the organization's stakeholders and affected groups such as community members, customers, and employees. In addition, the system provides a channel allowing people to respond to the company's messages. With mass notification systems, the value of intranet sites is increased: crisis managers can enter messages into the system and ask the mass notification system to reach the target audience group through the assigned channels.

Crisis response strategies are also an important area of practice for public relations practitioners. PR practitioners have to develop the different messages that are sent to various publics, providing responses that are quick, accurate and consistent. A quick response may not have much "new" information but it can help the organization position itself as a source allowing it to begin to present its side of the story. Carney and Jorden (1993) indicate that a quick response is active and shows an organization is in

control (p. 34). Arpan and Rosko-Ewoldsen (2005) conducted a study that documented how a quick, early response allows an organization to generate greater credibility than a slow response. Providing accurate information is also important when an organization communicates with its publics. When a crisis hits an organization, people want to know what happened and how that event might affect them. Only by providing accurate information makes an organization look consistent.

In the post-crisis phase, the organization is returning to business as usual. The crisis is no longer the focal point of management, but still requires some attention. Follow-up communication is also extremely important at this stage. Crisis managers must remember to deliver the additional information that they promised to provide to the public during the crisis. This is the first form of follow-up communication. The second form of follow-up communication requires the organization to release updates on the recovery process, corrective actions, and/or investigations of the crisis. Missing these actions could potentially make the public lose trust in the company, question the company about not taking responsibility to the public, and become part of the publics' negative history of the company. Also, the post-crisis phase is the time for recovering, reviewing, doubting, and analyzing the company. In this stage, a crisis manager should perform a crisis management evaluation. Evaluation reveals hard experience to the organization and must be remembered as a part of the institutional memory (Coombs, 1999, p. 161). Crises have a cyclical nature, drawing lessons from the former crisis management and making these experiences become the light of the oncoming crisis will help the organization to perform better while facing the next challenge.

In order to minimize the damage of the crisis and turn the crisis into an opportunity, instead of learning the crisis response strategies, an organization should do its best to prepare for one. Crisis management includes efforts designed to prevent and to detect potential crises, and to learn from crisis experiences (Caponigro, 2002; Cohn, 2000; Coombs, 1999b; Mitroff, 2001). The "image repair" and "situational crisis communication theories" are two approaches to managing crises.

Image Repair

Image repair is part of the post-crisis communication management phase. To decrease the level of damage caused by a crisis, a company uses a series of image repair operations to control the situation. According to Howard (1998), the value of a good corporate image comes from three aspects: financial value, marketplace value, and human resource value. There are a lot of advantages to a company which has a strong corporate image (p. 3). First, having a good reputation makes it easier for a company to attract and recruit the talents to grow the business and to develop deeper customer relationships. Second, a positive cooperate image reduces the recruitment costs. Furthermore, it can use its reputational assets to develop another brand without needing to build trust from customers again. The company's image can be altered or damaged by the accusations, complaints, and behavior of others. At the same time, the image can also be repaired by communication. Benoit and Pang (2007) stated that the key to understanding image repair efforts is to understand the nature of the accusations, attacks, or complaints that threaten corporate images (p. 244).

According to Benoit's image repair model (1995), to cope with crises and respond to image threats, image repair theory focuses on the content of the communication message and offers five broad categories of image repair strategies which are denial, evasion of responsibility, reducing offensiveness of event, corrective action, and mortification. Compensation is the final subcategory identified by Benoit and Pang (2007) for reducing offensiveness. It involves the compensation of the victims with a certain amount of goods, money, or services depending on the seriousness of the situation, so that the victims' dissatisfaction can be balanced. Generally speaking, if the compensation is acceptable to the victim, the firm's image should be restored, sometimes even improved (Benoit & Pang, 2007). Finally, Benoit and Pang's image repair model (2007) cite mortification as admitting to the wrongdoing, apologizing for the act, and asking for forgiveness (Benoit, 1999; Benoit & Pang, 2007). Among these strategies, "bolstering and corrective action have been proven to be effective strategies in earlier studies (Brinson and Benoit, 1999), and pleading defeasibility (the lack of the necessary knowledge to make informed decisions) also proved to be effective" (Benoit & Pang 2007, p. 258).

According to Coombs (1999) the image repair theory provides a several strategies for dealing with a crisis. It supplies ploys to deal with crises. Coombs also regards Benoit's image repair theory (1995) as taxonomy, which is just a subjective description. Coombs used quantitative research methods to combine crisis situations and strategies to conclude on reputational.

Historical Development of SCCT

Situational crisis communication theory (SCCT) has gone through a number of changes since first appearing as a decision flowchart in 1995. The historical development is divided into terminological changes, research-driven changes, and theory testing.

Changing the language of crisis theory was the first step in signifying the shift from symbolic to situational crisis theories. The term symbolic was chosen because the crisis response strategies were viewed as *symbolic resources* that could be employed during a crisis. Symbolic was replaced with situational because the theory is premised on the crisis situation. Research-driven change is the most significant change resulting from the tests of SCCT was the reconfiguration of crisis types from a grid to a continuum. Theory testing was the final component of the development of SCCT. To test SCCT, measures had to be developed for the central concepts of organizational reputation, crisis responsibility, and potential supportive behavior (Coombs, 1998, 2000b; Coombs & Holladay, 2001).

Organizational reputation, which focuses on trust, is a central concept in past and current conceptualizations of reputation. Crisis types may include organizational misdeeds, human-error accidents, technical-error accidents, technical-error recalls, workplace violence, and product tampering. An organization's crisis history has been found to have a significant effect on organizational reputation for all types of crises except technical-error recall crises. It has also been found to have a significant effect on

crisis responsibility for all types of crises except product tampering and technical-error recall crises (Coombs, 1998, 2000b; Coombs & Holladay, 2001). A crisis type determines the level of an organization's responsibility toward the crisis. There is also a negative correlation between crisis responsibility and organizational reputation.

The crisis situation will generate particular attributions of crisis responsibility, the degree to which the organization is perceived to be responsible for the crisis event. A list of reputation repair strategies by itself may have little utility to an organization undergoing a crisis. Managers have to explore when a specific reputation repair strategy or combination of strategies should be used (Coombs, 2007, p. 9). For this reason, attribution theory is a good concept for developing guidelines of reputation repair strategies. The attribution theory states that people try to explain why events happen, especially events that are sudden and negative. Indeed, attributions generate emotions and affect how people interact with those involved in the event. When the crises are negative, people either blame the organization in crisis or the situation. If people blame the organization, anger is created and people will react negatively toward the organization. Three negative reactions to attributing crisis responsibility to an organization have been documented: (1) increased damage to an organization's reputation; (2) reduced purchase intentions and; (3) increased likelihood of engaging in negative word-of-mouth (Coombs, 2007b; Coombs & Holladay, 2006).

Most of the research has focused on establishing the link between attribution of crisis responsibility and the threat to the organization's reputation. A number of studies have proven this connection exists (Coombs, 2004a; Coombs & Holladay, 1996;

Coombs & Holladay, 2002; Coombs & Holladay, 2006). Attribution of crisis responsibility is also an indicator of how much of a threat the crisis is to the organization's reputation and what crisis response strategies are necessary to address that threat. The crisis situation is a combination of a crisis type and the threat intensifiers. It can either be in the form of victim crises, accident crises and preventable crises. From the foundation of crisis type, the crisis manager uses the threat intensifiers to complete the crisis threat assessment. The threat intensifiers serve to intensify the reputation damage a crisis type can inflict on an organization and include [1]crisis history, [2]relationship history, and [3]severity.

Crisis response strategies are the firm's strategies of responding to media and publics during the crisis. SCCT works from a list of ten crisis response strategies that are grouped into three postures; deny posture, diminish posture and deal posture. A posture represents a set of strategies that share similar communicative goals and vary in terms of their focus on protecting the crisis victims (victim-orientation) and taking responsibility for the crisis. The three postures represent the three basic communicative options available to the crisis manager and reflect attribution and neoinstitutinal theory. Deny posture represents a set of strategies that claim that either no crisis occurred or that the accused organization has no responsibility for the crisis. If there is no crisis, there can be no organizational responsibility for a crisis (attribution theory) and no violation of legitimacy (neoinstitutional theory). Diminish posture reflects a set of strategies that

1 Crisis history: It lists similar crises an organization has had in the past.
2 Relationship history: It indicates if the organization has had a record of good works or bad behavior.
3 Severity: It is the amount of damage inflicted by the crisis, including injuries, loss of lives, financial loss, and environmental destruction.

attempt to alter stakeholder attributions by reframing how stakeholders should interpret the crisis (attributional theory). Deal posture includes the concern strategy that is an expression of compassion. The group shows that an expression of concern is viewed very similarly to apology and regret, the two crisis response strategies that can open an organization to legal liability. One valuable aspect of any theory is that it provides an organizing framework for the various concepts it uses. Based on this aspect, it is useful to place the various concepts from SCCT into a model that shows their relationship to one another.

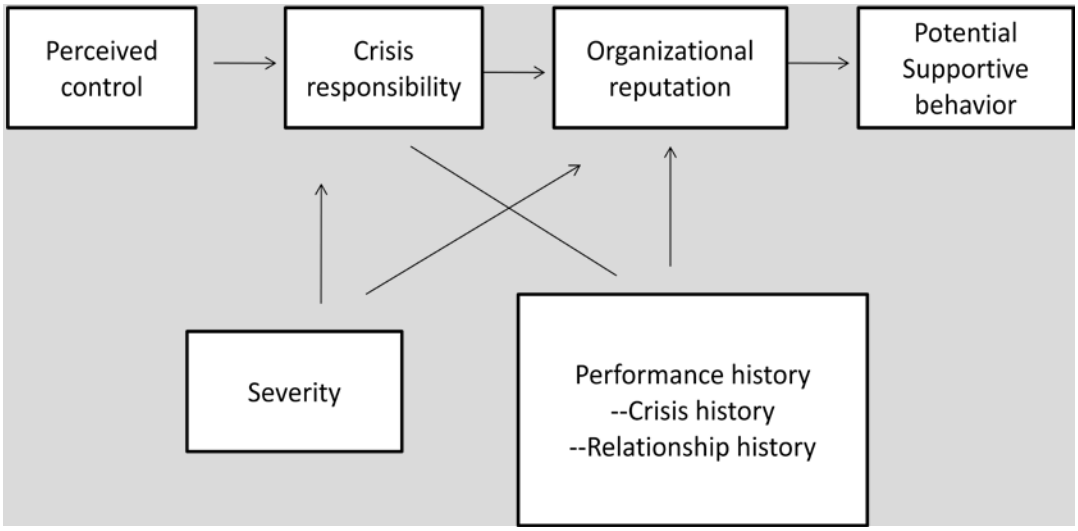
SCCT argues that crisis managers have to match their reputation repair strategies to the reputational threat of the crisis situation. Crisis managers should use increasingly accommodative the reputation repair strategies as the reputational threat from the crisis intensifies (Coombs & Holladay, 1996; Coombs, 2007b).

Situational Crisis Communication Theory

Situational crisis communication theory (SCCT) was introduced by Coombs in 1995. He pioneered the application of attribution theory to crisis management in public relations literature. It builds on Weiner's attribution theory (1986) which explained how people make causal attributions. SCCT articulates the variables, assumptions, and relationships in a crisis situation. It holds that crisis managers should consider these in advance when selecting crisis response strategies to protect an organization's reputation. SCCT is premised on matching the crisis response to the level of crisis responsibility attributed to a crisis. This study explores one of the basic assumptions of SCCT by

assessing whether the predicted correlation relationship between crisis responsibility and organizational reputation occurs across a range of crisis types. Results support the theory's predictions and suggest ways to refine the theory.

Figure 3-1 Situational Crisis Communication Theory Model



Source: Coombs, W. T. (2004)

To explain this model, the various relationships in SCCT are presented as propositions. Organizational reputation proposition and the attributions of crisis responsibility have a strong effect on perceptions of organizational reputation. Potential supportive behavior proposition is a strong, positive correlation exists between organizational reputation and potential supportive behavior, intentions to engage in acts that would help an organization. The severity proposition means severity has a significant intensifying effect on crisis responsibility and may damage to organizational reputation. Crisis history proposition means if an organization has an unfavorable crisis history, it may effect on the crisis responsibility and damage the organization's

reputation. Relationship history proposition can be divided to two parts. The first is an unfavorable relationship history, and it has a significant intensifying effect on crisis responsibility and damage to the organizational reputation. In contrast, the second part is a favorable relationship history. A favorable history has a significant reducing effect on crisis responsibility and damage to the organizational reputation. Both crisis history and crisis severity can determine the perception that whether an organization is responsible for the crisis or not. The crisis response strategy selection proposition indicates an organization will suffer less reputational damage from a crisis and experience greater potential supportive behavior if they match the crisis response strategy to the reputational threat of the crisis. The last step in SCCT is to match crisis situations to crisis response strategies and limitations. SCCT maintains that as attributions of crisis responsibility and/or the threat of reputational damage increases, crisis managers must use crisis response strategies that reflect a greater concern for victims and take more responsibility for the crisis.

Generally speaking, situational crisis communication theory is based on crisis communication, a subset of public relations. Botan's (1989) statement on the public relations field is a perfect fit for crisis communication today: "Theory does not develop automatically out of a large body of practical research. Systematic application of the theory development process is needed" (p. 107). In order to know the difference between "crisis communication theory (CCT)" and "situational crisis communication theory (SCCT)", the scope of each one must be clarified. Crisis communication theory emphasizes post-crisis communication and the use of crisis response strategies. This

includes what organizational leaders say and do after a crisis hits. It also emphasizes an organization's functions and management. However, situational crisis communication theory is interested in how crisis response strategies can be used to protect reputational assets after the presentation of instructing information[4], which is the first communication priority in a crisis. SCCT assumes the instructing information should have been disseminated in order to protect the people linked the crisis. It argues that the crisis situation determines which crisis response strategies will be the most effective in protecting the organization's reputation. In other words, it emphasizes the correlation between the crisis situation and the strategies. It states that crisis response strategies reflect a greater concern for victims and take more responsibility for the crisis.

Regarding the use of crisis response strategies, CCT focuses on what organizational leaders should respond and react after a crisis hits; however, SCCT more focuses on how crisis response strategies can be used to protect reputational assets after the presentation of instructing information (Sturges, 1994, p. 297). Besides, SCCT assumes that the instructing information has been disseminated in order to protect people linked to the crisis. As far as the functions are concerned, CCT only repairs the image, which has been harmed by crises and rescues the reputation of the organization; however, SCCT determines which crisis response strategies will be the most effective in protecting the organization's reputation. It not only rescues but also enhances the reputation from the public. The strategies CCT applies are: denying responsibility, hedging responsibility, ingratiation, making amends and eliciting sympathy. The method that

[4] Instructing information: Tells stakeholders what to do to protect themselves from the crisis, the basics of what happened, and what the organization is doing to fix the situation and to prevent a recurrence of the problem.

SCCT proposes for dealing with crises involves analyzing situation first, and then selecting different strategies from the attribution theory and situational crisis communication theory. There are four types of crisis response strategies suggested by SCCT: deny, diminish, rebuild and reinforcing. Deny strategies include claiming there is no crisis (denial); trying to prove the organization has no responsibility for the crisis (scape-goating), or attacking the accusers. Diminish strategies attempt to minimize the organization's responsibility (excuse) or the seriousness of the crisis (justification). Rebuild strategies involve providing compensation or making apologies to the public for the crisis. Reinforcing strategies involve reminding stakeholders about past good works (bolstering) or praising stakeholders (ingratiation). According to SCCT, reinforcing strategies must be used with one of the other three strategies.

Furthermore, SCCT argues that crisis managers have to match their reputation repair strategies to the reputational threat of the crisis situation. Crisis managers should use increasingly accommodative the reputation repair strategies as the reputational threat from the crisis intensifies (Coombs & Holladay, 1996; Coombs, 2007b). Crisis managers can follow a two-step process to assess the reputational threat of a crisis. The first step is to determine the basic crisis type. This means crisis managers have to consider how the news media and other stakeholders are defining the crisis. Coombs and Holladay (2002) had respondents evaluate crisis types based on attributions of crisis responsibility. They distilled this data to group the basic crises according to the reputational threat each one posed (p. 280). Figure 3-2 provides a list the basic crisis types and their reputational threat.

Figure 3-2 Crisis Types by Attribution of Crisis Responsibility

Crisis Types by Attribution of Crisis Responsibility
Victim Crises: Low Crisis Responsibility Natural disasters: Acts of nature such as tornadoes or earthquakes. Rumors: False and damaging information being circulated about an organization. Workplace violence: Attack by former or current employee on current employees onsite. Product/Tampering/Malevolence: External agent causes damage to the organization.
Accident Crises: Moderate Crisis Responsibility Challenges: Stakeholders claim that the organization is operating in an inappropriate manner. Magadamage: A technical accident where the focus is on the environmental damage from the accident. Technical breakdown accidents: A technology or equipment failure causes an industrial accident. Technical breakdown recalls: A technology or equipment failure causes a product to be recalled.
Preventable Crises: Strong Crisis Responsibility Human-error accidents: Industrial accident caused by human error Organizational misdeed: Management actions that put stakeholders at risk and/or violate the law.

Source: Coombs; W. T. (2007)

The second step is to review the intensifying factors of crisis history and prior reputation. If an organization has a history of similar crises or has a negative prior reputation, the reputational threat is intensified. A series of experimental studies have documented the intensifying value of crisis history (Coombs, 2004a) and prior reputation

(Coombs & Holladay, 2001; Coombs & Holladay, 2006; Klein & Dawar, 2004). The same crisis was found to be perceived as having much strong crisis responsibility (a great reputational threat) when the organization had either a previous crisis (Coombs, 2004a) or the organization was known not to treat stakeholders well/negative prior reputation (Coombs & Holladay, 2001; Coombs & Holladay, 2006; Klein & Dewar, 2004). Figure 3-3 is a set of crisis communication best practices derived from attribution theory-based research in SCCT (Coombs, 2007b, Coombs & Holladay, 1996; Coombs & Holladay, 2001; Coombs & Holladay, 2006).

Figure 3-3 Attribution Theory-based Crisis Communication Best Practices

1. All victims or potential victims should receive instructing information, including recall information. This is one-half of the base response to a crisis.
2. All victims should be provided an expression of sympathy, any information about corrective actions and trauma counseling when needed. This can be called the "care response." This is the second-half of the base response to a crisis.
3. For crises with minimal attributions of crisis responsibility and no intensifying factors, instructing information and care response is sufficient.
4. For crises with minimal attributions of crisis responsibility and an intensifying factor, add excuse and/or justification strategies to the instructing information and care response.
5. For crises with low attributions of crisis responsibility and no intensifying factors, add excuse and/or justification strategies to the instructing information and care response.
6. For crises with low attributions of crisis responsibility and an intensifying factor, add compensation and/or apology strategies to the instructing information and care response.
7. For crises with strong attributions of crisis responsibility, add compensation and/or apology strategies to the instructing information and care response.
8. The compensation strategy is used anytime victims suffer serious harm.
9. The reminder and ingratiation strategies can be used to supplement any response.
10. Denial and attack the accuser strategies are best used only for rumor and challenge crises.

Source: Coombs; W. T. (2007)

In general, a reputation is how a stakeholder perceives an organization and it is a valuable, intangible asset for an organization. However, the threat posed by a crisis extends to behavioral intentions as well. From Coombs's early research (2007b), it is

suggested that lessons designed to protect the organization's reputation will help to reduce the likelihood of negative word-of-mouth and the negative effect on purchase intentions as well. SCCT is an increasingly influential theory in crisis communication research. It assumes an organization's reputation is a valuable resource that can be seriously damaged by any crisis. Effective crisis management can minimize the damage and may allow an organization to emerge stronger than it was before the crisis.

To summarize the guidelines provided by SCCT, the concerned crisis response strategy should be added to any crisis with victims, in order to express compassion for the victims at a loss. SCCT maintains that as attributions of crisis responsibility and/or the threat of reputational damage increases, crisis managers must use crisis response strategies that can reflect a greater concern for victims and take more responsibility for the crisis. SCCT allows crisis managers to understand the effect of choosing a non-matching strategy by indicating why the effectiveness of the response is reduced. SCCT therefore helps crisis managers to protect reputational assets effectively.

Research Questions

In this study, situational crisis communication theory will be reviewed by analyzing the TJX crisis in 2007. Through analyzing 75 of the news reports which covered TJX crisis and response, this study will answer the research questions by using quantitative results and qualitative results, the study tries to answer the following questions:

RQ1: Could the situational crisis theory be useful in dealing with the information technology crisis as TJX?

RQ2: What strategies, if any, worked in the TJX breach information case in responding to the crisis?

RQ3: Could situational crisis theory have helped TJX deal with this crisis more successfully?

CHAPTER 4

METHODOLOGY

The methodology employed in this research paper used is case study. Content analysis is used to support and complement the analysis. According to Stacks (2002), "There is no more descriptive approach to public relations than the case study" (p. 71). A good case study can describe and analyze a person, organization or event in detail.

Qualitative Method

Qualitative research methods were developed in the social sciences to enable researchers to study social and cultural phenomena. This form of research aims to gather in-depth understanding of the research questions, and explore the reasons behind the results. In short, it investigates the why and how of decision making in a situation and helps to focus the findings. There are various approaches to qualitative research methods: (a) Participation in the setting; (b) Action research; (c) In depth interviews; (d) Analysis of documents and material; (e) Focus groups; (f) Case-study research. Qualitative data sources include observation and participant observation (fieldwork), interviews and questionnaires, documents and texts, and the researcher's impressions and

reactions (Myers, 1997, p. 241). The reason the case study research method was chosen for this paper is that "Qualitative research is a highly useful in policy and evaluation research, where understanding why and how certain outcomes were achieved is as important as establishing what those outcomes were" (Bryman, 1988, p. 160).

Case Study Research

Case study is an ideal methodology when a holistic, in-depth investigation is needed (Feagin, Orum and Sjoberg, 1991). It is one sort of qualitative research methodology and an extension of secondary research. The methods involve an in-depth, longitudinal examination of a single instance or event (case). According to Bent (2006), "As a result the researcher may gain a sharpened understanding of why the instance happened as it did, and what might become important to look at more extensively in future research. Case studies lend themselves to both generating and testing hypotheses" (p. 220). Therefore, case study can be a single case or multiple case studies, it also includes a few notions of quantitative evidence, relies on multiple sources of evidence. The purpose of case study, cited by Hartley (2004, p. 323), "is to provide an analysis of the context and processes which illuminate the theoretical issues being studied."

Researcher Robert K. Yin defines the case study research method as an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used (Yin, 1984, p. 23). The goal of most case studies is to describe and provide examples. A secondary goal is to provide a grounded theory of how public relations work. "Case study research is the most common qualitative method

used in information systems " (Orlikowski and Baroudi, 1991; Alavi and Carlson, 1992). According to Yin (1989), the case study methodology is used when: (1) the study questions are "how" or "why" questions, (2) the researcher has little control over the event, and (3) when a contemporary phenomenon or an event with a real-life context case study is emphasized. The TJX case is qualified with the above reasons. Hartley (2004), states that a case study is particularly fitting to questions that require detailed understanding of social or organizational processes (p. 28).

Hartley (2004) also specifically points out seven types of questions that a case study methodology can be used to address: "(1) how the organizational and environmental context impacts or influences social processes; (2) for exploring new or emerging processes or behaviors; (3) exploring not typicality but unusualness or extremity with the intention of illuminating processes; (4) capturing the emergent and changing properties of life in organizations; (5) where exploration is being made of organizational behavior which is informal, unusual, secret or even illicit; (6) to understand everyday practices and their meanings to those involved, which would not be revealed in brief contact; and (7) to perform the essential in cross-national comparative research" (p. 325).

According to Stacks (2002), "Case studies are in-depth studies of particular people, organizations, events, or even processes. They provide a richly detailed and complete understanding of the case under study" (p. 71). The advantage of case study method is that what is under study has already occurred. The researchers are able to use current evidences to analyze and explain what and why the case occurred, or in the case

of public relations, how the public relations practitioners managed the outcome. Case studies provide details that can only be found in hindsight and presents them in such a way as to establish what strategies worked and why. Thus, the case study in public relations can examine the way a problem was stated and the initial research gathering stages based on environmental scanning and monitoring; the strategic communication planning based on stated objectives; the communications themselves, the actual outputs; and the evaluation of the entire program or campaign (Stacks, 2002, p. 68). On the other hand, the disadvantage of case study is that it is not able to generalize its findings. Case study is not able to do this because it is an in-depth analysis of a particular phenomenon; however, it provides examples of what worked and what did not work in a specific case. The purpose of the case study methodology, cited by Hartley (2004), is to provide an analysis of the context and processes which illuminate the theoretical issues being studied.

The case study was selected as methodology in this instance since it is particularly suited for answering research question. In order to obtain rich detailed information in this case, it was necessary to engage the case study methodology. By collecting news and information from newspapers, magazines, online articles and newsletters from the TJX's website, this study uses a timeline approach to analyze the events and the data in detail. The timeline presents the key dates and processes TJX engaged in, in dealing with the crisis. Finally, the case study provides a richness of data and understanding that is not available through other methods. This research paper will use case study as the main methodology for the purpose of understanding how TJX dealt with the crisis in 2007.

Since the crisis is rich with real-life contexts, and the case study research is the most suitable methodology to use.

Content Analysis

Qualitative content analysis has been defined as "a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns" (Hsieh & Shannon, 2005, p. 1278). Neuendorf (2002) offers a six-part definition of content analysis: "Content analysis is an in-depth analysis using quantitative or qualitative techniques of messages using a scientific method, including attention to objectivity-intersubjectivity, a priori design, reliability, validity, generalizability, replicability, and hypothesis testing and is not limited as to the types of variables that may be measured or the context in which the messages are created or presented" (p. 10).

Content analysis is also called documentary analysis or informational analysis. The characters of content analysis are "subjective" and "systematic". Content analysis allows the public relations researcher to employ some sophisticated statistical analyses on qualitative data. Berelson (1952) defined "content analysis" as a systematic, replicable technique for compressing many words of text into fewer content categories based on explicit rules of coding (p. 135). D.P. Cartwright (1953) defined the process of content analysis as, "We propose to use the terms "content analysis" and "coding" interchangeably to refer to the objective, systematic, and quantitative description of any symbolic behavior" (p. 466). And D. Hays (1969) thought the linguistic foundation is the

basic for a theory of content analysis (p. 57). In 1990, Dane regarded content analysis as a research method used to make objective and systematic inferences about theoretically messages (p. 170).

Content analysis is a method for summarizing any form of content by counting various aspects of the content. The content can be from newspapers, magazines, documents, and journals. Lasswell (1952) and Holsti (1968) indicated the six elements of Content Analysis: (1) Who--who is the source of information; (2) What--what is the content; (3) Whom--who is the information receiver; (4) How--How to communicate--the skill of communication; (5) With what effect---What is the effect of this information, and (6) Why--The reason of communication about this information. Wildemuth & Zhang (2006) stated that the goal of content analysis is to identify important themes or categories within a body of content, and to provide a rich description of the social reality created by those themes/categories as they are lived out in a particular setting. Through careful data preparation, coding, and interpretation, the results of qualitative content analysis can support the development of new theories and models, as well as validate existing theories and provide thick descriptions of particular settings or phenomena.

For this study, news articles from United States, England, Canada and China covering the TJX information leak crisis were examined. The materials collected were published between January 17, 2007 and March 12, 2010. A total of 75 news articles were collected from newspapers, on-line news, magazines and announcements posted on the TJX website. The researcher organized the articles by publication date and coded them from 1 through 75. The researcher coded for the publishing date, word count,

number of information sources, information sources, and quotes from TJX spokesmen or company newsletters. The positions from the articles were classified as either positive, negative, or neutral.

After all units were recorded, each of the news sources was assigned a specific number for coding. The sources of information were divided into 11 types: TJX's newsletter, TJX's spokeswoman Sherry Lang, TJX executives including the ex-CEO and current CEO, the spokesman Bruce Spitzer for the Massachusetts Bankers Association, spokesperson for Visa Card, spokesperson for MasterCard, spokesperson for Citizen's Bank, the information technology analysts, Federal Trade Commission (FTC), and the Florida Department of Law Enforcement and government. Content of the quotes was classified into 10 categories, which were (1) Explanation of the reasons why the breach crisis happened, (2) TJX investigations and its estimations of the financial loss, (3) The cooperation with the security companies to solve the crisis (4) the settlement with banks, (5) Assurance of customers safety while shopping in TJX, (6) Apologies to the public, (7) Explanation of the late announcement of the breach crisis, (8) The method used by TJX in dealing with the customers during the crisis, (9) The amount of compensations, and (10) others. With the coded information, the data was keyed into the Statistical Package for the Social Sciences (SPSS) software to get the mean, median, frequency, and percentage numerical values. This enabled the researcher to evaluate whether the company's procedure for dealing with the crisis was successful or not, according to SCCT. It also helped to reveal what crisis communication strategies were conducted, and how these strategies were conducted.

Content analysis enables researchers to look at qualitative data in a quantitative manner. By using content analysis method to support case study for this research, the information from the TJX case was systematically collected and analyzed. After defining the variables which influence the replying strategies, the results will serve to reveal better recommendations that might have been used by TJX in dealing with the crisis.

CHAPTER 5

RESULTS

Through the analysis of 75 news reports which cover the TJX crisis and response, this study will answer the research questions using the qualitative results and also supported by the quantitative method. The research questions are:

RQ1: Could the situational crisis theory be useful in dealing with the information technology crisis as TJX?

The analysis of the 75 news reports that directly discussed the TJX breach crisis, yielded the following results.

All of the news came from a total of 16 sources including TJX website. The Register news (44%), PC World news (14.6%) and the TJX Company (13.3%) were the main sources of news coverage for the crisis.

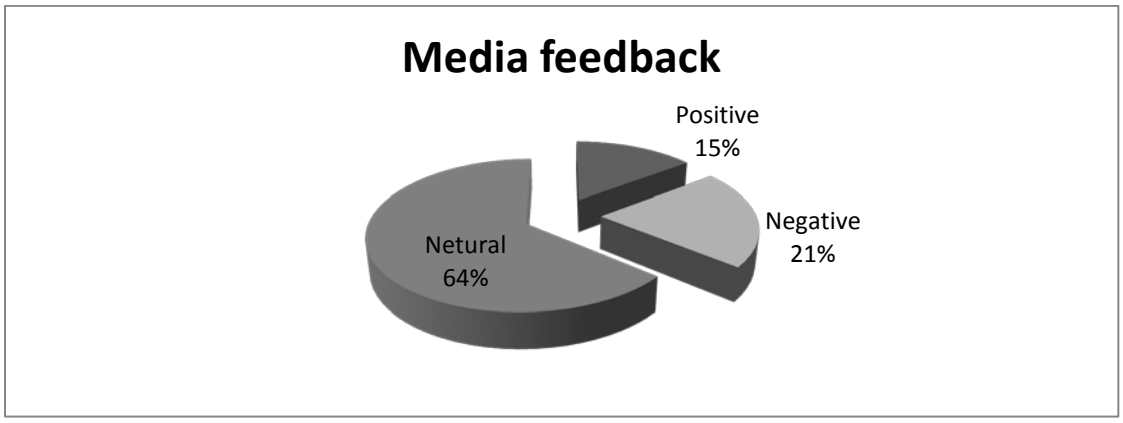
A closer look at the results also revealed that TJX's newsletter and company statements were the most frequently used sources, cited in up to 58 articles. TJX spokeswoman Sherry Lang was quoted 14 times, making her statement the second most

frequently used source, with Bruce Spitzer, a spokesman for the Massachusetts Bankers Association being the most quoted. Both TJX's ex-chairman, Ben Cammarata, and current president Carol Meyrowitz who took the responsibility of updating the media, were quoted 11 times each. Other sources included Massachusetts Bankers Association, banks statement from companies such as Visa, MasterCard, Citizen's Bank, information technology analysts, Federal Trade Commission, Florida Department of Law Enforcement and government. In general, TJX was the major source of information and accounted for up to 77% of sources in the news or articles.

11 articles (14.6%) held a positive attitude toward TJX breach information crisis, 16 articles (21.3%) took a negative position, and most of articles (48) took a neutral position (64%), only reporting news to the public.

In a crisis, an organization cannot expect the media to report positively; however, it could influence the media to report in a neutral position to reduce the harming reputation. By providing instructing and adjusting information when crisis occurred, TJX minimized the problem it faced. These results therefore answer the first research question indicating that the situational crisis theory was applicable in the information technology crisis as TJX.

Figure 5-1 Media Feedback toward TJX Crisis



RQ 2: What strategies, if any, worked in the TJX breach information case in responding to the crisis?

By examining the quotes from TJX in each article, this study is able to answer the second research question. Crisis response strategies include what an organization says and does after a crisis happens. An analysis of the quotations from the company during the crisis, reveal that information about the investigation appeared 33 times. Quotes about solving problems appear 23 times. TJX is seen giving information about its cooperation with IBM and other security companies to strengthen its information security. The next category has to do with explaining the reasons why this breach crisis happened. In this category by TJX was quoted 16 times. The settlement with banks about compensation appeared 14 times, with quotes being available from 2008 until 2010. Quotes about "the dealing method TJX used" and "clarifying the current safety of shoppers' information" were both used 12 times. Quotes on regret and apology from the

CEO appeared 9 times. Next on the descending list of frequency, which both appeared 8 times, were quotes providing explanations of the late announcement about breach crisis" and "the amount of compensation toward customers.

Based on SCCT, these response strategies help an organization to protect reputation. According to the frequency of the quote contents, there are five strategies that were used by TJX, these are corrective action, minimization, mortification, shift the blame, and compensation. The results, shown in Figure 5-2, indicate that corrective action strategy was used the most and worked well. Minimization, shift blame, mortification and compensation strategies are also worked and played important roles in TJX's case.

Figure 5-2 Quote Frequency and the Corresponding strategies

Corresponding strategy	**Quote content**	**Times**	**Percentage**
Corrective Action	Investigate and estimated results	33	17.2%
Corrective Action	Solving way (cooperate with IBM and security company)	23	11.9%
Corrective Action	Explain the reason why the breach crisis happened	16	8.3%
Minimization	The settlement with banks	14	7.3%
Minimization	The dealing methods TJX used (ex: set the toll-free help lines)	12	6.3%
Minimization	Clarify the current safety	12	6.3%
Mortification	Regret and apology from the CEO	9	4.7%
Shift the blame	Explanation of the late announce	8	4.1%
Compensation	The amount of compensation	8	4.1%
	Others (Opinions from MBA, other banks, security companies and the government)	57	29.7%
Total		**192**	**99.9%**

As SCCT argues, the effectiveness of communication strategies is dependent on the characteristics of the crisis situation. This study analyzes the situation and tries to figure out what strategies TJX used that matched SCCT. SCCT states that the company

facing a crisis has to analyze situation first, then, chose the right response toward the crisis. Analyzing the situation helps an organization to determine an appropriate response. The reputational threat is assessed by a two-step process. The first step is to identify the crisis type. A crisis type is the frame used to interpret the crisis (Lerbinger, 1997). The second step is to determine whether there is a crisis history, whether or not an organization has experienced similar crises.

SCCT research has shown that a history or similar crises intensifies the reputational damage of a crisis (Coombs & Holladay, 2001). Crisis types and crisis history are combined to determine the reputational threat of a crisis situation. Determining the crisis type provides an initial assessment of the reputational threat by indicating the level of crisis responsibility associated with the crisis. By reviewing the situation TJX faced, the crisis may be classified as a moderate reputational threat since it involved a technical breakdown, which might be considered an accident. The level of threat is an important element because it drives the selection of crisis response strategies for the organization. In this crisis type level, it means the organizational actions leading to the crisis were unintentional. After knowing the level of threat, the crisis managers may then examine the company's crisis history.

Research on the TJX Cos., revealed that TJX did not have any similar crises in its history. For crises with low attributions of crisis responsibility (accident crises) and no history of similar crises, SCCT suggests that crisis managers use the diminish crisis response strategies. Diminish strategies attempt to minimize the organization's responsibility and the seriousness of the crisis. There are two actions involved in this

strategy, which are excuse and justification. The excuse strategy can help crisis mangers minimize organizational responsibility by denying intent to do harm and/or claiming inability to control the events that triggered the crisis.

A review of the case shows that TJX's response was a mix of diminishing and rebuilding[1] strategies. For diminish, TJX attempted to highlight its current safety inspection process and minimize the severity of the information breach that had occurred. It asserted that "TJX is continuing its investigation seeking to determine whether additional customer information may have been compromised" (TJX announcement, January 17, 2007); and "TJX has hired IBM and General Dynamics to help investigate and improve its security (Security Focus, March 30, 2007)". To rebuild its reputation amongst customers and banks, TJX implemented mortification and compensation tactics. The company made apologies through its website and sent videos to the news media. Quoted from The Boston Globe (January 28, 2007), Ben Cammarata, TJX's ex-CEO, stated "I regret any difficulties our customers may experience because of this incident, and we want our customers to feel safe shopping in our stores and I really believe you are." And to restate the apology, the current CEO, Carol Meyrowitz, said "Let me begin by telling our customers personally how much I regret any problems or inconvenience they may have experienced as a result of the unauthorized intrusion into our computer system (TJX newsletter, February 21, 2007)." Both quotes reveal the mortification strategy used by TJX. For compensation, TJX made settlements with banks and

[1] Rebuilding strategies, compensation and apology, are suggested to be used in the crises with low or strong attributions of crisis responsibility and a history of similar crisis.

companies such as Visa, MasterCard and Massachusetts Bankers Association, and paid about 256 million as part of a settlement agreement. To customers, TJX promised that all the affected customers would be reimbursed for the replacement costs of their drivers' licenses. Also, the customers who had to change bank and credit card information would receive vouchers redeemable in any TJX stores. In addition, TJX held a special event for all customers whether they were affected by the crisis or not. Quoted from ComputerWorld (September 24, 2007), "victims will receive vouchers redeemable in TJX stores in the U.S, Canada and Puerto Rico, and TJX will hold a one-time, three-day customer appreciation event at which it will offer a 15 percent discount on all goods sometime next year." Based on the results from research question two, this study tries to answer the next research question: It addresses how situational crisis communication theory might have helped TJX deal with crises more successfully.

RQ3: How can situational crisis communication theory help TJX deal with the crisis more successfully?

SCCT holds that the effectiveness of communication strategies is dependent on the characteristics of situation. First of all, an organization can analyze situation, and then select the right response toward the crisis. Knowing the situation helps an organization to determine an appropriate response aimed at the public (Coombs, 1999). SCCT agrees that crisis mangers can use a combination of crisis response strategies. An examination of this case reveals that TJX used both diminish strategies and rebuild strategies.

The company used corrective action by providing solutions to the problems caused. It also used a minimization strategy in entering into settlements with banks and credit card companies. By doing so, TJX dealt with the crisis successfully in the beginning. From TJX newsletters and news reports from the media, the quote "TJX has been working aggressively with relative firms as IBM and Federal government to monitor and evaluate the intrusion, assess possible data compromise, and seek to identify affected information (TJX announcement, January 17, 2007)" indicates that the company used corrective action of the rebuild strategies. The quote "We immediately engaged two leading computer security and incident response firms to investigate the problem and enhance our computer security in order to protect our customers' data (Computerworld Security newsletter, January 17, 2007)" also indicates the use of the corrective action and minimization strategy. Also, the quote "I regret any difficulties our customers may experience because of this incident, and we want our customers to feel safe shopping in our stores and I really believe you are (The Boston Globe, January 28, 2007)" showed the use of the mortification strategy.

When facing criticism from banks and media about the delayed announcement of the crisis, the quote "by delaying a public announcement, with the help of top security experts, we were able to contain the problem and further strengthen our computer network to prevent further intrusion. Therefore, we believe we were working in the best interests of our customers" (Boston Herald, January 29, 2007) showed use of the justification approach from the diminish strategy. The quote "Some banks and payment card companies have advised us that they have found what they consider to be

preliminary evidence of possible fraudulent use of credit payment card information that may have been stolen from us, but they have not shared with us the details of their preliminary findings (PC World, March 21, 2007)" indicates the use of the shift blame strategy.

In conclusion, TJX conducted the crisis response strategies in a sufficient and moderate way. Other than the strategies above that TJX used, excuse under diminish strategy should have been used to some extent in this case, as suggested by SCCT. More discussion about the steps and strategies TJX should have used in addition will be presented in the next chapter.

CHAPTER 6

DISCUSSION

Results from the statistics and analyses of the news reports that are presented above, TJX communicated with the public through the media and implemented a crisis management program. This case study was analyzed based on the situational crisis communication theory (SCCT), which is premised on matching the crisis response to the level of crisis responsibility attributed to a crisis. SCCT emphasizes that an organization should match the situation and crisis in order to select the most appropriate and beneficial reaction to help it deal with a crisis (Coombs, 2007). This theory holds that the effectiveness of communication strategies depends on: first, identifying the situation an organization is facing ; second, determining whether there is a crisis history, which refers to whether an organization has experienced similar crises or not; last, selecting the right response toward the crisis.

This case study found that TJX used a mix of diminishing and rebuilding strategies such as corrective action, minimization, mortification, shift the blame and compensation to respond the public and media. Corrective action, as a rebuild strategy, was the most effective crisis communication strategy in the TJX case. The corrective

actions undertaken by the company included; cooperating with other security companies to investigate the intrusion and strengthening its computer systems to prevent similar crises from happening. Quotes about "the investigation and estimated results" from TJX category appeared 33 times," occupied 17.2% in TJX's response. This proves the value and effectiveness of this strategy. TJX availed to the public, their plan to reduce reputational harm and also expressed their concerns about the occurrence. The concern crisis response strategy should be added to any crisis with victims in order to express compassion for the victims. TJX gave all victims or potential victims instructing information, and showed an expression of sympathy. By making apologies to the public and showing concern, TJX won the back the loyalty of the customers. This was shown by the fact that the breach crisis did not influence TJX's revenue on sales. Information about corrective actions and showing concern are necessary when an organization faces a crisis.

Shifting the blame strategy was used when TJX explained the reason why they announced the breach crisis late. The targets for the blame were the banks and payment card companies since, according to TJX; they had not shared the information about the cards which may have been used fraudulently. Shifting the blame is useful when the target is blame-worthy. In this case, the strategy was particularly useful because both TJX and the credit cards companies were victims. The credit card companies did not fully cooperate with TJX and may have caused TJX to announce the breach late. The shifting the blame strategy helped the audience to accept TJX's late announcement about the information security breach.

By reviewing the situation TJX faced, it can be deducted that TJX was under moderate reputational threat, since the crisis was a technical breakdown accident. TJX could not control the intruders and the organizational actions leading to the crisis were unintentional in this crisis type. Besides, an organization's reputation is built from its history, whether similar crisis exists or not. Research found out that TJX did not have similar crisis history. With no similar crisis history, and technology broken accident crisis type, the TJX case could be categorized as one with low attributions.

In this crisis situation, diminished strategies should have been used more extensively by TJX. This is because TJX was in a low responsibility situation. Diminished strategies include; excuse and justification, attempt to minimize the organization's responsibility and the seriousness of the crisis. TJX could add excuse and justification strategies to the instructing information and care response. For example, TJX could state "TJX did not intend for the crisis to occur and that accidents could happen in the day to day operations of any organization." By including these strategies TJX could also further guarded its reputation and relieved the public's concerns. The excuse strategy could have also helped crisis mangers minimizes organizational responsibility by denying intent to do harm and claiming inability to control the events that triggered the crisis. In other words, diminish posture is the role the TJX should have taken more since it reflects a set of strategies that attempt to alter stakeholder attributions by reframing how stakeholders should interpret the crisis.

The most important thing in dealing with crisis is the crisis response strategies must reflect a greater concern for victims and take more responsibility for the crisis. In

this case, TJX did not disclose the breach immediately, and what sort of information was compromised specifically. TJX initially held off for months in reporting the breach because there was an investigation under way; however, a public relations practitioner is required to be honest and transparent in letting all parties know what the situation is. Being honest is the best position for companies and public relations practitioners to take. For crises with minimal attributions of crisis responsibility and no intensifying factors as the TJX case, instructing information and care response is sufficient. TJX should have provided information and announced the breach crisis as soon as possible, even of this meant notifying the government and law enforcement agencies in order to strengthen their computer network security. Although the result of providing this information might harm an organization's reputation and cause drop in, it also builds customers' confidence toward an organization.

Furthermore, in SCCT, it is suggested that an organization uses its own website to release news and communicate with the public and stakeholders (Taylor and Kent, 2007). This is because during a crisis, the stakeholders and news media will turn to the Internet to get information. Communication with the stakeholders is an important undertaking, especially during a crisis. This is because stakeholders play a crucial role in the settlement of an organizational crisis. By using newsletter posts on the organization's website, TJX managed to control the news source and clarify the position it held on the matter. TJX did well by posting announcements on its website, as this helped to solidify good relations as well as boost communication with share holders a time when they were concerned about the financial implications of the crisis. Regarding minimization

strategies, TJX has made a settlement with banks and Massachusetts Bankers Association to have their credit back, and it set up toll-free lines to help customers who were concerned and worried. TJX used compensation strategy not only toward banks by making payments, but also covered costs caused by the breach for the affected customers. Two years later, it offered 15 percent discount in their stores to all customers in three countries. Compensation is an effective strategy which can be used anytime when victims suffer serious harm. However, TJX should have offered the 15 percent discount event earlier, right after crisis happened, not two years later. The late offer may have made customers feel that the company did not show enough concern and respect at the time of the crisis.

Best Practices in Crisis Communication

Crisis management is a critical organizational function. Good crisis communication can be widely used to improve organizational and professional practice. Lack of proper crisis communication can result in serious harm to stakeholders or losses for an organization. For this reason, effective crisis management is required to handle all threats. Generally speaking, the primary concern in a crisis has to be public safety, not only to a tangible body but also to an intangible asset. Failure to address public safety may intensify the damage from a crisis. To enhance the function of crisis communications, the public relations practitioners should address the following aspects.

First, crisis communicators have to help the public overcome fear of the crisis and guide them into a positive attitude toward the companies. Questions of blame and

responsibility are inevitable in crises for companies and therefore crisis managers should divide responses by issues of accuracy, timeliness, useful information and the need to help victims and make them have confidence in the companies. Second, by matching reputation repair strategies to the reputational threat of the crisis situation, crisis managers are able to deal with crisis and win back reputation effectively. In addition, crisis managers have to assure the public that all available information can be delivered correctly not only through press releases but also through intranet sites. An intranet site provides a direct approach that allows employees, suppliers and customers to access relevant information. Having a crisis website is the best practice during a crisis since the website plays a function for the organization as a formal source to present crisis information. It can also prevent an organization's words from being twisted by attackers or the media. By communicating and using newsletter posts on an organization's website, companies can control the news source and have a better way to communicate with employees, stakeholders and the public.

Last but not least, communication strategies and response strategies should be fully integrated into the decision-making process. The crisis response is what a crisis communicator does and says after the crisis hits, and the messages are sent to various publics. Crisis managers have to listen to the public's concerns carefully so that they can know exactly what the public's needs are. In the beginning of the crisis, if crisis managers promise to provide additional information, they have to make sure they follow through on those promises, or they may face the risk of losing the public's trust. In addition, the organization needs to release updates on the recovery process, corrective

actions and investigations of the crisis. The follow-up information and communication that are required depend on the amount of information promised during the crisis and the time the company takes to complete the recovery process. At the end, the effective crisis response strategies and methods are not only to protect and rescue an organization's reputation but also enhance the reputation from the public.

Limitations

For the characteristics and disadvantages of case study, this research has the following limitations. First of all, part of the information is not directly obtained from the practitioners of TJX or other involved parties. Most of the information may not be truly accurate and perhaps contains some biases. For example, one of the news reports claims that the law enforcement officials in Florida arrested six individuals suspected while other reports indicate the suspects were eight. Media bias is another limitation of this study. Reporters might add their own opinions to the news and this could be the reason why some reports hold positive attitudes toward TJX's information breach crisis while some lean toward the negative. Second, TJX's case is just a single case study that belongs to one type of crises so that the conclusion of this study may not be generalized or fit with other cases.

The next limitation is the lack of integrity of the organizational data. All the organizational data is from TJX's Website. TJX may only provide the positive and embellished information so that the public can only get the data which will benefit TJX. In addition, the results of this study are concluded by observation from the collected

reports and information. There is no formal interview or survey to prove the publics' satisfaction of TJX's crisis responses, neither if the company's reputation is influenced by the strategies it applied. Lastly, there may be other reasons to influence the results of the evaluation but there is no way to determine and discover this because of the limited information.

Recommendation for Future Study

There are numerous case studies discussing how companies deal with technology crises. The issue of managing a company's information technology (IT) has become increasingly complex and important. Therefore, to set up a database of how to deal with crises about IT broken is continuously needed and requires more studies to enrich it.

This case study used collecting data and content analysis to analyze the research. The majority of data were collected from newspapers and company's website. The opinions were based on the news reporters and official statements from TJX. During the present study, samples of customers' feedback were not collected. Clearly, there is a need to add survey or interview to see whether the affected customers were satisfied on TJX's responses and actions. Then, it could prove the selected responding strategies suggested by situational crisis communication theory were effective on this case.

Besides, the future study can also test other strategies matching on different crisis situations. Currently, companies and crisis managers are used to applying crisis communication theory into crisis responses to deal with crisis. However, crisis responses are related with companies' past history and crisis situation. For this reason, situational

crisis communication theory (SCCT) is another better choice for companies and makes SCCT differ from other approaches to crisis management.

In this case, the type of crisis was accident, which means TJX took moderate crisis responsibility of it. Since TJX is in a low attribution of crisis responsibility and there is no similar crisis in its history, SCCT suggests TJX adds excuse and/or justification strategies to the instructing information and care responses. Other than the accident crisis situation and above type of responses, there are two more crises types (victim, preventable) and three more strategies suggested by SCCT deny, rebuild and reinforcing strategies. Researchers can study different cases and analyze whether the strategies SCCT suggested are effective or not. Crises have numerous natures and results in different responding strategies. Therefore, further research can utilize situational crisis communication theory in different crisis cases.

Conclusions

TJX faced the network intrusion in December 2006, and updated officials of banks and law enforcement on January 3, 2007. Then, it notified the public about breach information on January 17, 2007. In total, TJX had lost 45.7 million credit and debit card numbers and personal information related to almost 500,000 people in this crisis. In 2009, TJX and attorney generals from 41 states made an agreement that TJX has to pay 97.5 million dollars as a settlement cost, which covered the reissued card costs and potential liability. Including the compensation to banks and the costs for consultants,

security upgrades, attorney fees and damage-control marketing, it is estimated TJX might spend $1 billion on this breach crisis.

Due to the advanced technology, firms deliver information and save important data via internet or computers. While technology has made peoples lives much easier, it has also created much vulnerability. This means that organizations should pay closer attention to internet security for protecting critical information. This case study recommends retailers be concerned about the security of their information technology systems and protect customers' information from theft and fraudulent use. The TJX crisis is evidence that information technology security remains fragile at some retailers. From this case study, it helps firms to pay more attention to databases security and provides potential solutions for dealing with such crises.

Situational crisis communication theory (SCCT) states that the effectiveness of communication strategies is dependent on the characteristics of a situation. An organization should select the right response toward the crisis after analyzing situation it faces. By understanding the situation first, an organization can determine appropriate responses to the public. According to SCCT, TJX's crisis type is an accident crisis and it is in a low attribution of crisis responsibility. Knowing the exact crisis situation enables crisis managers choose a matching strategy. By indicating the effectiveness or right responses based on situation, SCCT helps organizations to protect reputational assets and deal with crises efficiently.

To conclude, TJX conducted the crisis response strategies in a gradual and moderate manner. Investigating the computer intrusion, cooperating with other security companies, apologizing to the public, making settlement with banks, and compensating its customers are among the strategies TJX used. TJX's reactions and response strategies helped the company deal with the crisis and save its reputation. Ultimately, crisis management is designed to protect an organization and its stakeholders from threats and reduce the impact felt by threats. An organization should seek any way to improve prevention, preparation, and the responses toward crisis. The SCCT is able to help an organization to increase the effectiveness of crisis communication.

REFERENCES

All business. Retrieved from http://allbusiness.com

Arpan, L.M., & Roskos-Ewoldsen, D.R. (2005). Stealing thunder: An analysis of the effects of proactive disclosure of crisis information. *Public Relations Review 31(3),* 425-433.

Augustine, N. R. (1995). Managing the crisis you tried to prevent. *Harvard business Review,73(6),* 147-158

Basline Magazine. Retrieved from: http://baselinemag.com

Benoit, W.L. (1997). Image repair discourse and crisis communication. *Public Relations Review, 23(2),* 177-186.

Benoit, W.L. & Pang. A. (2008). *From theory to practice, Crisis communication and image repair discourse*. Pearson Allyn & Bacon, Boston, 244–261.

Bent, F. (2006). Five misunderstandings about case-study research. *Qualitative inquiry, Vol. 12*, 219-245.

Berelson, B. (1952). *Content Analysis in Communication Research*. Glencoe, Ill: Free Press.

Boston.com business. Retrieved from: http://Boston.com/business/articles

Botan, C. H. & Hazleton, V. (2006). *Public Relations Theory II*. Lawrence Erlbaum

Associates.

Business Weekly Magazine. Retrieved from: http://www.businessweekly.com.tw

Brewerton. P. & Millward. L. (2001). *Organizational research Methods.* London: SAGE.

Bryman, A. (1988). *Quantity and Quality in Social Research*. London: Unwin Hyman.

Carney, A., & Jorden, A. (1993). Prepare for business-related crises. *Public Relations Journal 49,* 34–35.

Channelregister.co.uk. Retrieved from: http://channelregister.co.uk

Chong, K. S. (2004). "Six Steps to Better Crisis Management" *Journal of Business Strategy* 25, 43-46.

Coombs, W. T. (1995). *The development of the situational crisis communication theory* (D. N. Bonita, Ed.). Boston: Pearson.

Coombs, W.T. (1995). Choosing the right words: The development of guidelines for the selection of the 'appropriate' crisis-response strategies. *Management Communication, 8(4),* 447-476.

Coombs, W. T. (1999). Information and compassion in crisis responses: A test of their effects. *Journal of Public Relations Research, 11(2),* 125.

Coombs, W. T. & Holladay, S. J. (1996). Communication and attributions in a crisis: An experiment study in crisis communication. *Journal of Public Relations Research, 8(4),* 279-295.

Coombs, W. T. (1998b). An analytic framework for crisis situations: Better responses from a better understanding of the situation. *Journal of public relations research, 10(3),* 177-191.

Coombs. W. T. (1999). *Ongoing crisis communicatio*n. London: Sage.

Coombs, W. T. (2004). Impact of past crises on current crisis communication: Insights From situational crisis communication theory. *Journal of business communication, 41, July*, 265-289.

Coombs, W. T. & Heath, R. L. (2006). *Today's Public Relations.* New York: A Division of Guilford Publications, Inc.

Coombs, W.T. (2007b). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10,* 1-14.

Corporate Leadership Council. (2003). *Models and methodologies for on-boarding programs*. Washington, DC: Corporate Executive Board.

Dean, D. H. (2004). Consumer reaction to negative publicity: Effects of corporate reputation, response and responsibility for a crisis event. *Journal of business communication, 41*, 192-211.

Denzzin, N.K. (1982). Contributions of anthropology and sociology to qualitative research methods" *Qualitative Methods for Institutional Research* Ed. Kuhns, Eileen and Martorana, S. V. (CA: Jossey-Bass Inc), 17-26

Dilenschneider, R. L. (1991). Marketing communication in the post-advertising era. *Public relations review, vol. 17*, 227-236.

Dilenschneider, R. L. (2000). *The corporate communications bible: Everything you need to know to become a public relations expert*. Beverly Hills: New Millennium.

Epoch Times. Retrieved from: http://tw.epochtimes.com

Fearn B. K. (1996). *Crisis Communications: A Casebook Approach.* New York: Lawrance Erlbaum Associate.

Feagin, J., Orum, A., & Sjoberg, G. (Eds.). (1991). *A case for case study*. Chapel Hill, NC: University of North Carolina Press.

Fink, S. (1986). *Crisis Management: Planning for the Inevitable*. IUniverse, 2000.

Hartley, J. (2004). "Case study research" *Essential Guide to Qualitative Methods in Organizational Research Ed*. Cassell Catherine and Symon Gillian. London: SAGE.

Hendrix, J. A. (1998). *Public Relations Cases, 4th ed.* Belmont, CA: Wadsworth.

Howard, S (1998). *Corporate Image Management: A marketin discipline ofr the 21st Century*. Butterworth-Heinemann Asia.

The Register news. Retrieved from: http://theregister.co.uk

TJX newsletter. Retrieved from: http://tjx.com

Klein, J. & Dawar, N. (2004). Corporate social responsibility and consumers' attributions of brand evaluations in product-harm crisis. *International journal of marketing, 21*, 203-217

Lerbinger, O. (1997). *The crisis manager: facing risk and responsibility*. NJ: Lawrence Erlbaum. Maxwell, A. D.

Lisbeth, B. (2009). *Industry Immersion Learning: Real-Life Industry Case-Studies in Biotechnology and Business*. Weinheim: Wiley-Blackwell.

Myers, M. D. (1997). Qualitative Research in Information Systems. London: Chapman & Hall.

Neuendorf, K. A. (2002). *The content analysis guidebook.* Chicago: Sage.

Neuman, W. L. (2000). *Social research methods: Qualitative and quantitative approaches*. Thousand Oaks: Sage Publications

NNBP Mapper. Retrieved from: http://mapper.nndb.com/

PC World news. Retrieved from: http://pcworld.com

Stacks, D. W. (2002). *Primer of Public Relations Research.* NY, New York: A Division of Guilford Publications, Inc.

Stemler, S. (2001). An overview of content analysis. *Practical Assessment, Research & Evaluation, 7(17).* Retrieved May 1, 2009 from: http://PAREonline.net/getvn.asp?v=7&n=17

Sturgers, D. L. (1994). Communicating through Crisis: A Strategy for Organizational Survival. *Management Communication, 7*, 297-316.

Taylor, M., & Kent, M. L. (2007). A taxonomy of crisis response on the Internet. *Public Relations Review 33*(2), 140–146.

Ulmer, R.R., Sellnow, T.L., & Seeger, M.W. (2006). *Effective crisis communication: Moving from crisis to opportunity.* Thousand Oaks: Sage

Wildemuth, B. M., & Zhang. Y. *Qualitative Analysis of Content.* Retrieved from: http://www.ils.unc.edu/~yanz/Content_analysis.pdf

World Journal. Retrieved from: http://www.worldjournal.com

Yin, R. (1984). *Case study research: Design and methods* (1st ed.). Beverly Hills, CA: Sage Publishing.

Yin, R. (1989). *Case study research: Design and methods* (Rev. ed.). Newbury Park, CA: Sage Publishing.

Yin, R. (1993). *Applications of case study research*. Newbury Park, CA: Sage Publishing.

APPENDIX

Timeline of TJX information breach case

2006/ 12/19

- TJX found out the network intrusion

2007/ 1/3

- TJX informed officials of banks and law enforcement about intrusion

2007/1/17

- TJX announced it may have exposed card data in four countries to the public
- TJX released a limited number of customers whose driver's license information was stolen from the compromised systems

2007/1/21

- TJX' CEO made apology to the public

2007/1/30

- Lawsuit filed against TJX by Massachusetts Bankers Association

2007/2/21

- TJX updated information for computer systems intrusion on its newsletter

2007/3/14

- Federal Trade Commission investigated TJX's data leak case

2007/4/26

- Lawsuit filed against TJX by banks

2007/9/24

- TJX Offered settlement to the customers

2007/11/30

- TJX made the settlement agreement with Visa

2007/12/3

- TJX agreed to pay banks $41 million to cover Visa's losses

2007/12/18

- TJX made the settlement agreement with Bankers Associations

2008/4/2

- TJX made the settlement agreement with MasterCard

2008/5/14

- TJX completed the previous announcement of settlement with MasterCard

2009/1/22

- TJX offered 15 percent discounts in all TJX stores for customers

2009/6/23

- TJX made the settlement with attorneys general