Communications of the Association for Information Systems

Volume 34 Article 50

2-2014

The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis

Anat Hovav
Korea University - Korea, anatzh@korea.ac.kr

Paul Gray
Claremont Graduate University

Recommended Citation
Hovav, Anat and Gray, Paul (2014) "The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis," *Communications of the Association for Information Systems*: Vol. 34 , Article 50.
DOI: 10.17705/1CAIS.03450
Available at: https://aisel.aisnet.org/cais/vol34/iss1/50

Communications of the Association for Information Systems

CAIS

The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis

Anat Hovav

Korea University Business School, Seoul Korea

anatzh@korea.ac.kr

Paul Gray

Claremont Graduate University

Abstract:

While unfortunate physical events result in a negative market reaction, cyber events rarely do. It is our contention that a security attack is a complex intervention that ripples through the attacked company's ecosystem. Over time, new information about the incident is revealed which might change the trajectory of the effect. This study aims to understand the impact of a security breach on the attacked company, its ecosystem (e.g., consumers, vendors, banks, and hackers), and surrounding society. By utilizing a stakeholder analysis as a methodological framework, we found that, while some stakeholders are losers, other are winners. Our analysis also implies that, depending on subsequent events, the effect of a security breach on the attacked firm varies over time, suggesting a "wait and see" attitude by the market.

Keywords: security breach impact, TJX case, stakeholder analysis, event study, longitudinal study

Editor's Note: The article was handled by the Department Editors for Information Technology and Systems

Volume 34, Article 50, pp. 893-912, February 2014

"Drop a pebble in the water:
just a splash, and it is gone;
But there's half-a-hundred ripples
Circling on and on and on,
Spreading, spreading from the center,
flowing on out to the sea.
And there is no way of telling
where the end is going to be."

~By James W. Foley~

I. INTRODUCTION

Whereas adverse physical events result in negative market reaction (see Appendix A), cyber events such as security breaches rarely have a statistically significant negative impact. Studies that examined the effect of security incidents on the market value of companies have found mixed results. Several reasons were cited for these inconclusive results, such as: (1) lack of awareness by investors [Hovav and D'Arcy, 2003], (2) researchers combining various firm sizes [Cavusoglu, Mishra, and Raghunathan, 2004], and (3) lack of proper classification of breaches [Hovav et al., 2007]. In addition, unlike physical events that are constrained to a single company, product, or physical location, cyber attacks transcend organizational and geographic boundaries, increasing their potential reach. It is our contention that the effect of cyber attacks is not contained within the focal company but is likely to ripple throughout the company's ecosystem.

Generally, an intervention in any system is likely to generate a ripple effect. The consequences depend on the group and its relationships to the source of the intervention [Grimble and Wellard, 1997]. Large-scale security breaches such as ChoicePoint.com [Laudon and Laudon, 2007] or the TJX case (the subject of this article) are complex and involve a large number of stakeholders and innocent bystanders, some of whom are winners and some of whom are losers. The outcome of the ripple effect can be zero-sum or positive sum on the collection of stakeholders and on society.

In addition, prior studies examined the market reaction to security breaches immediately after the breach was discovered. However, over time, new information about the company's reaction to the attack, the actual damage, consumer churn, and potential legal consequences come to light. This new information might change the impact of the attack on the focal company and its stakeholders. A longitudinal in-depth analysis of a major incident might shed light on the long-term effect of information security incidents.

In this article, we describe the TJX Companies Inc. breach in terms of its effect on the company and its stakeholders, the perceived risks involved, and the extent of the effects over a period of several years. We use stakeholder analysis (SA) as a tool to investigate the perceived risk resulting from one security breach (i.e., TJX) from the perspective of the company and its stakeholders over time.

II. THE IMPACT OF CYBER BREACHES

Prior research on the impact of security breaches has been inconclusive. For example, Hovav and D'Arcy [2003] found that Denial of Service (DOS) attacks had little overall effect on the stock price of the companies attacked. However, DOS attacks did have a larger impact on "Internet-centric" companies than on non-Internet companies. Hovav and D'Arcy [2004] found that the impact of computer virus announcements on the stock price of attacked companies also was insignificant, particularly in the long run. Other studies [Anthony et al., 2006; Cavusoglu et al., 2004] that examined the impact of various security breaches on the market value of firms found only a minor effect, mostly limited to e-commerce companies. These results are surprising considering the sizeable reported economic effect of security breaches [Richardson, 2007].

One major difference between a physical incident and a cyber breach is the "reality of the damage." When a physical event happens, the damages are clear. A damaging fire destroys all or part of a building. An oil or chemical spill directly or indirectly destroys the environment. However, cyber security attacks are different. For example, a company might suffer a DOS attack, which may be real, but the damages are not binary. That is, the hacker may

use the DOS attack to interfere with the operation of the website where the loss depends on the extent of the interference and the length of time the site is down. Or a hacker may try to extort money from a company and will allow restoring normal operation only after the money is paid. A DOS attack against an e-commerce company might result in tangible losses (loss of purchases, loss of customers), while the same type of attack against a non-Internet company may result only in inconvenience and potential intangible losses (loss of brand name or trust).

Physical incidents are also geographically limited. Thus, two widely separated fires are unlikely to be correlated, whereas cyber events may be correlated regardless of their origin or their intended target. As discussed later, several supposedly unrelated incidents were connected to the TJX event. However, that information was unavailable at the initial time of discovery.

Net Calculated Risk

Most previous studies of cyber risk calculated only the risk accrued by the attacked companies. The present study recognizes that other entities can be, and are, affected by the attack. These entities include both stakeholders and innocent bystanders. For example, in the TJX case we found that Wal-Mart was affected indirectly.

Another basic assumption is that information security attacks always create a negative effect. However, as we will show, information security attacks can have negative effects on some stakeholders and positive effects on other stakeholders. The old axiom, that "it is an ill wind that blows nobody any good," still holds true. One can logically assume that an attack that exposes stakeholders' private information will negatively affect the attacked company. It may also be true that an attack on company X will have a positive impact on its competition if customers switch to the competition. However, Ettredge and Richardson [2001] showed that a set of DOS attacks had a negative spillover effect. That is, competitors exhibited financial losses due to the reported attacks.

Yet, other stakeholders are likely to gain from an attack. For example, Dranove and Olsen [1994] found that in some product recall cases, the main cost is not for the repair but rather for advertising and notifying customers. In such an event, advertising agencies, newspapers, television, and radio stations are likely to gain, as are lawyers, auditors, and IT and security consulting firms. Since most of these firms operate in the same market as the attacked company, the *net calculated risk* for the event is an important economic quantity (see below). In short, the impact of the attack depends on the stakeholders involved.

III. STAKEHOLDER ANALYSIS

Stakeholder analysis has been used as a methodology for the study of systems in various disciplines, including Management Information Systems (MIS) (e.g., Pan, 2005; Gallivan, 2001). SA is often used by identifying key players and investigating their interests in the system [Grimble and Wellard, 1997]. SA literature divides stakeholders into two categories:

- active (those who affect the system)
- passive (those who are affected by the system)

In the case of hacking attacks, stakeholders also may be transitional. A hacker, for example, is an active stakeholder who has an interest in her target company for the duration of the attack. Once the attack is over, the "relationships" are severed.

CSR Dimensions and Their Application to Information Security

A branch of study related to SA is Corporate Social Responsibility (CSR). CSR research examines the interaction between the organization and its external environment. The theory of the firm states that the main objective of managers is to maximize returns and shareholders' value [Jensen and Meckling, 1976]. Thus, managers are expected to engage in activities that maximize profits; any activity that does not directly improve organizational profitability is in conflict with shareholders' interests.

Alternative theories such as SA and CSR state that organizations are responsible not only to their shareholders, but also to other stakeholders including society as a whole. CSR theory began in the 1950s [Carroll, 1999]. The main thrust of CSR is that organizations should balance economic benefits with social responsibility. Social responsibility is defined in various ways in the literature from ethical behavior [Johns, 1995] to environmental consideration [Russo and Fouts, 1997]. One of the most common CSR definitions used was introduced by Carroll [1979]: "*The social responsibility of business encompasses the economic, legal, ethical, and discretionary expectations that society has of organizations at a given point in time*" [Carroll, 1979, p. 500].

Carroll's definition corresponds to Martin's [2002] definition of *instrumental* and *intrinsic* acts. Specifically, the economic and legal aspects correspond to the instrumental acts while the ethical and discretionary aspects correspond to the intrinsic acts. Ethical behavior is defined often by code of conduct, industry standards, and best practices. Ethics are not mandated by regulatory agencies, yet businesses and managers are expected to adhere to them. The discretionary dimension deals with actions that are not required or expected. Organizations perform discretionary acts to be viewed as a "good corporate citizen" or because of social norms. CSR theory was applied to a large number of domains such as human resources (including MIS professionals), environmental issues, and the welfare of developing countries.

Maintaining users' private information can be described as a CSR act. For example, in some cases it is an instrumental act because the lack of privacy and security is shown to be a major obstacle in the development of consumer-related electronic commerce [Miyazaki and Fernandez, 2001; Earp, Anton, Aiman-Smith, and Stufflebeam, 2004] leading to loss of potential rent. In other cases, it is instrumental because the company operates in a regulated industry (e.g., healthcare). Alternatively, maintaining customers' confidentiality could be regarded as an ethical act. For example, companies such as TJX that maintain credit card information are expected to follow industry standards (i.e., the PCI[1]). This standard is not a government mandate and does not carry judicial penalties. However, it is a common practice. The ethical element of information confidentiality is more pronounced in recent times since consumers have become quite concerned with how organizational practices lead to loss of private information (e.g., Stewart and Segars, 2002; Metzger, 2004).

Waddock and Graves [1997] and Posnikoff [1997] found a positive correlation between CSR behavior and a firm's financial performance, while Cochran and Wood [1985] found only a slight positive relationship between CSR and financial performance. McWilliams and Siegel [2001] assert that the relationship between CSR and financial performance depend on organizational characteristics. A meta-analysis of fifty-two studies and over 33,000 observations by Orlitzky, Schmidt, and Rynes [2003] concluded that CSR behavior does have a positive relationship with a firm's financial performance. Unlike prior research that addressed only the effect of a security breach on the firm and only on or shortly after the day of the attack, in the next sections we discuss two additional types of impact. The first is the affect of the breach on the ecosystem of the attacked firm. The second is the impact of the attack on the target company over the length of the incident.

For a given stakeholder at the time of the attack, the risk is a function of the relative size of the attack compare to the actor's income, risk appetite, company size, and industry. For example, a small company with relatively low net income has less sustainable slack resources to defend against a very large cyber attack. A large company can absorb the costs of such an attack without risking major financial strain.

$$\textbf{Risk}_{\textbf{stakeholder i}} \textbf{ = f (relative-attack-size, p(attack), f(CSR), } \varepsilon \textbf{)} \quad (1)$$

For all stakeholders combined, the total risk is the sum of the individual risks for all stakeholders.

$$\textbf{Total risk = f (}\Sigma \text{ Risk}_{\text{stakeholder i}}\textbf{)} \quad (2)$$

Because some stakeholders may gain while others may lose from a given attack, the overall risk can be zero-sum.

In addition, the value of the stolen information is likely to diminish over time, and so is the impact of the attack until there is another event (or news) relevant to the initial attack. The new event or information will change the perceived risk for a certain set of stakeholders or will introduce a new stakeholder into the equation. For example, if a hacker steals credit card information from a company and does not use the credit card numbers for, say, three to four weeks, the impact of the attack diminishes and eventually disappears. However, if several weeks later it is discovered that merchandise was bought using these credit card numbers, the negative impact of the attack changes for the company attacked and only for those individuals whose credit cards were actually used. Therefore, over time, we are looking at a step-function, as illustrated in Figure 1. The time intervals are not necessarily equal. Rather, they depend on the occurrence of events. Intervals also can overlap. The level of impact also varies from one interval to the next. Overlap is likely to happen closer to the initial attack since news regarding the attack appears more often. However, the level of impact is not necessarily time-dependent. A major event (say a year after the attack), such as an out-of-court settlement, could have a larger (positive) impact than a minor event (say a month after the initial attack), such as discovering the mode of the attack.

[1] https://www.pcisecuritystandards.org/tech/index.htm

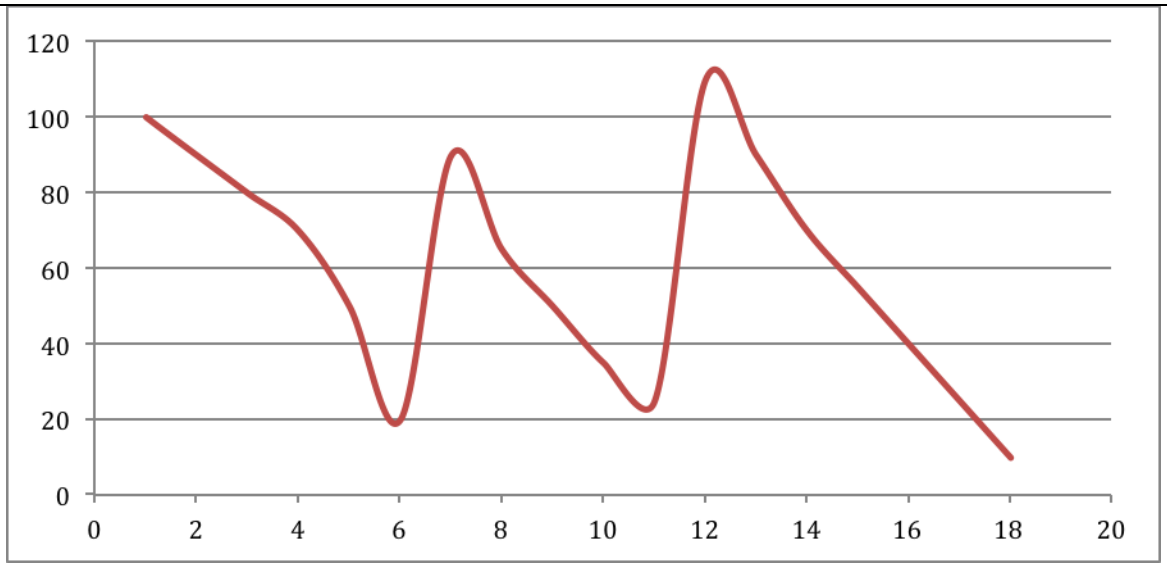

Figure 1. Financial Impact over Time

In the following sections, we will describe the case of TJX and use a stakeholder analysis to examine the effect of the attack on TJX's ecosystem. We will also employ an event study methodology to analyze the market reaction to the post-attack events over time. We begin by detailing the chain of events that lead to the discovery of the attack.

IV. THE CASE OF TJX

To investigate the components of a given attack, we selected a security breach which was reported as "the largest online burglary ever," namely, the TJX attack[2,3]. In addition to its size and impact, the attack involved criminal hackers and a breach of private information. The exposure of private information has been classified as a high impact attack [Hovav, Andoh-Baidoo, and Dhllion, 2007]. Our goal is to examine the impact of an attack on TJX over time and the impact of the TJX attack on several of its stakeholders. The sequence of events is described in Table 1.

Company Profile

The TJX Companies Inc. (ticker TJX) is headquartered in Framingham, Massachusetts, and is a global off-price retailer of apparel and home fashion. TJX operates over 2,400 stores in the United States, Canada, and Europe. TJX owns companies such as T.J. Maxx, Marshalls, A.J. Wright, Winners, T.K. Maxx, HomeGoods, HomeSense, and Bob's Stores. T.J. Maxx is the largest off-price retailer in the U.S. with 821 stores in forty-eight states, and Marshalls is the second largest off-price retail store with 734 stores in forty-two states. The retailer targets middle- to upper-middle-income shoppers. The TJX strategy is to sell brand-name merchandise for prices lower than department stores or specialty stores. TJX employs around 450 buyers who negotiate with around 10,000 vendors worldwide. The merchandise in the stores adjusts often and is based on an opportunistic buying strategy.[4] TJX companies pride themselves on their use of sophisticated inventory and distribution systems. For example: "highly automated storage and distribution systems track, allocate and deliver an average of approximately 11,000 items per week to each T.J. Maxx and Marshalls store" (10K reporting, p. 2). In general, TJX relies heavily on Information Technology to support processes such as pricing, markdown decisions, inventory replenishment, and timely distribution which are essential for the companies' off-price strategy. In December 2006, TJX discovered that it is being attacked by hacker(s). Table 1 details the timeline of the events surrounding the attack.

[2] http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1249421,00.html#

[3] The Target attack occurred while this paper was in the pipeline. Given the limited amount of verifiable information regarding the Target attack at the time of publication, we kept the above quote.

[4] Unlike most department stores which purchase their inventory a year in advance, TJX buyers purchase products for the current season. Most purchases are from the manufacturers directly.

Table 1: A Timeline of Events[5]	
Date	**Event**
July 2005	First breach—possibly started in Minnesota
September 2005	Second intrusion
September 2005	TJX plans to upgrade their wireless encryption.
October 2005	TJX begins upgrading their wireless encryption software.
November 2005	Fidelity Homestead (Louisiana savings bank) customers started noticing fraudulent transactions from Wal-Mart in Mexico.
January 2006	Fidelity Homestead discovers bogus purchases from various stores in California.
Fall 2006	$8 million worth of merchandise is purchased at various Wal-Mart stores in Florida.
May–December 2006	Third intrusion
September 29, 2006	TJX receives an audit report stating that they are not complying with Visa and MasterCard standards.
November 2006	Wal-Mart discovers $8M in fraudulent purchases.
December 18, 2006	An audit finds abnormalities in TJX card processing.
December 19, 2006	TJX hires IBM and General Dynamics Corp to investigate the problem.
December 22, 2006	TJX notifies the U.S. Secret Service and other law enforcement agencies of the breach.
December 26–27, 2006	TJX begins notifying banks and card issuers, FTC, SEC, etc.
Early December 2006	TJX notifies Canadian authorities.
December 19, 2006–January 17, 2007	Investigators try to catch the hackers in the act. TJX also is being investigated by the Privacy Commissioner of Canada.
January 17, 2007	TJX makes a public announcement of the breach and begins sending credit card lists to issuers.
January 19, 2007	The first set of class-action lawsuits is filed, followed by a number of lawsuits mostly in the U.S. and Canada.
January 2007	TJX completes the upgrade of their wireless encryption software.
February 21, 2007	TJX files a report that indicates a larger breach than initially thought (started earlier and of a larger scope).
October 24, 2007	The number of compromised cards may be as high as 94 million.[6]
October 29, 2007	Fifth Third Bancorp is fined $880,000 by Visa for its role in the TJX case.
November 30, 2007	TJX settles with Visa. Settlement agreement is $41 million.
March 27, 2008	TJX and FTC settle. No monetary penalty is imposed.
April 2, 2008	TJX settles with Master Charge. Settlement agreement is $24 million.

TJX notified the authorities (U.S. Department of Justice, U.S. Secret Service, and Royal Canadian Mounted Police) in mid-December 2006 and hired IBM and General Dynamics to investigate the breach. However, the first public announcement of the attack was released on January 17, 2007. Prior to the announcement, numerous banks in Massachusetts were alerted by Visa to replace thousands of credit cards. Only later it became clear that the fraudulent use of these stolen credit card numbers was the result of the TJX breach. The attack took place over two years. The initial count was approximately 46 million credit and debit card numbers and several thousand driver license numbers of customers that returned merchandise without receipts.[7] Later the count was raised to 94 million. Although many of the card numbers expired (about 75 percent) and many debit card numbers did not have corresponding PIN numbers, the attack was considered the largest in U.S. history at that time.

The technical details related to the attack are still sketchy. The following two paragraphs are based on a report from MSNBC.[8] MSNBC claimed that the hackers intercepted information traveling between wireless price check equipment and registers in some Marshall stores in the Miami area.[9] The wireless communication was not properly encrypted. TJX was using Wireless Encryption Protocol (WEP) rather than the more secure Wi-Fi Protected Access (WPA) protocol. TJX began converting all its WEP to WPA in 2004. However, with approximately 2,500 stores globally, the process took over two years. TJX claimed that they completed the conversion in time to remain in good standing with credit card associations such as Visa and MasterCard standards.[10] Using the data they captured, the

[5] Majority of the dates are from http://www.privcom.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp and from TJX 10K filing on March 28, 2007. Additional dates are extracted from various news and articles.
[6] http://www.msnbc.msn.com/id/21454847/from/ET/
[7] http://www.infoworld.com/article/07/01/17/HNtjxbreach_1.html
[8] http://www.msnbc.msn.com/id/20979359/
[9] Other reports point to stores in Minnesota.
[10] Based on a statement made by TJX spokeswoman Sherry Lang, http://www.theglobeandmail.com/servlet/story/RTGAM.20070926.wgttjhack0926/BNStory/Technology/

hackers broke TJX's encryption code and used that code to eavesdrop on employees as they logged in to TJX's central database, stealing user names and passwords. The hackers proceeded to create bogus user accounts, which they then used to steal millions of credit and debit card numbers over a span of a year and a half. The numbers were stored on approximately one hundred files set-up by the hackers. The hackers were so confident that they even left messages for each other on the TJX system. The stolen numbers were sold on password-protected websites to various groups that used them to create bogus credit and gift cards around the world. Unbeknown to the public or the authorities, this practice continued throughout the breach (from July 2005 until December 2006). It was only after TJX discovered the breach that many of these international bogus charges were linked to TJX.[11] The hackers cleaned most of the traces, files, and audit files from the system, thus making it difficult to trace the source of the attack.

According to the Canadian Privacy Commissioner Jennifer Stoddart's report in addition to using old security protocols, TJX retained customers' credit information for too long and did not mask sensitive information such as driver license numbers.[12] The report stated that the "retailer retained customer data years after it should have been purged, including driver license numbers collected when customers returned merchandise without receipts. Some of the stolen information was from transactions concluded as far back as 2002," but does not specify what the proper retention time should be. In summary, TJX security failed not only on the technical side, but also in establishing proper security policies. However, TJX officials claim that they followed Visa guidelines and requirements.

The Stakeholders

Intruders

Hacker culture literature differentiates among various intruders, such as hackers, crackers, script kiddies, and hacktivists, based on their intent, level of expertise, and code of conduct. Intruders do not always attack systems for financial gains. Often attacks are political, status-related, or a proof-of-concept. In the case of TJX, the attack was conducted by a well-organized team of professional cyber criminals strictly for financial gain. For the sake of brevity, we will use the term *intruders* to denote the attackers and *hacking* to denote their actions. In the initial stages of the investigation, investigators speculated that the methods used indicate that the hacking was done by a known group of organized crime members. The gang was suspected in several other hacking cases in the U.S.[13] Unlike prior cases, the intruders cleaned their tracks and did not boast their success on any known hackers' websites or blogs. The intruders also did not use the card numbers themselves. Rather, they sold them on the black market, suggesting that they are professional criminals. Several people were arrested in Florida and Turkey for using stolen credit card numbers. In June 2007, a number of Cuban nationals were arrested in Florida.[14] The arrestees produced counterfeit credit cards using some of the stolen numbers. The Florida group received the numbers from an Eastern European group. The ringleader pled guilty and received a five-year jail sentence and a $600,000 fine.[15] In August 2007, a Ukrainian national was arrested in Turkey for selling credit card numbers from the TJX theft.[16] Although authorities hoped that the Turkey arrest would lead to a break in the case, none of these arrests led to the capture of the masterminds behind the attack.

In August 2008, the U.S. Department of Justice charged eleven people in the TJX attack. Three of the intruders are U.S. citizens, the rest are from Estonia, Ukraine, China, and Belarus. The large number of diverse nationalities highlights the global nature of current professional cyber criminal teams.[17] Although charges were brought against eleven people, not all of them were caught immediately. For example, Sergey Valeryevich Storchark was arrested in India only in May 2010. Storchark was the reseller of the stolen data and on his way back to the Ukraine via Turkey when arrested. It is speculated that once he had returned to the Ukraine, it would have been impossible to extradite him.[18] Gonzales was charged for a number of attacks (including the TJX case), and after a plea bargain was sentenced to twenty years in jail. He is expected to be released in 2025. His four codefendants received anywhere from two to seven years sentences.[19] It is speculated that other members of the cyber criminal team involved in the TJX case, were not caught. The existence of hackers' "safe havens" creates difficulties in arresting and convicting cyber criminals.[20]

[11] http://online.wsj.com/article_email/article_print/SB117824446226991797-lMyQjAxMDE3NzA4NDIwNDQ0Wj.html
[12] http://www.msnbc.msn.com/id/20979359/, http://www.boston.com/business/technology/articles/2007/09/25/wireless_systems_faulted_in_tjx_theft/
[13] http://online.wsj.com/article_email/article_print/SB117824446226991797-lMyQjAxMDE3NzA4NDIwNDQ0Wj.html
[14] http://www.eweek.com/article2/0,1895,2156263,00.asp
[15] http://www.computerworlduk.com/management/security/cybercrime/news/index.cfm?newsid=5187
[16] http://www.infoworld.com/article/07/08/22/Turkish-make-arrest-in-TJX-data-breach-case_1.html
[17] http://www.infoworld.com/d/security-central/eleven-charged-in-massive-id-theft-scheme-511?page=0,1
[18] http://www.infoworld.com/d/security-central/another-hacker-arrested-tjx-data-theft-charges-853
[19] http://en.wikipedia.org/wiki/Albert_Gonzalez
[20] For example, see http://www.reuters.com/article/2013/08/01/us-usa-security-snowden-russia-idUSBRE9700N120130801.

Communications of the Association for Information Systems

Consumers

The most obvious stakeholders in this case are the consumers who buy TJX products. However, the assumption that all TJX consumers are losers is premature. We divide consumers into three categories:

1. Consumers who suffered identity theft as a result of the breach. This group suffered the largest damages—actual (financial) and punitive (emotional and loss of time). The total number of cases where the credit cards were used fraudulently is unknown, as is the amount of the losses incurred which were not covered by the credit card companies.[21]
2. Consumers whose credit card information was included among the stolen cards, but the information was never used for fraudulent purchases. Although these consumers did not suffer actual damages, they did suffer punitive damages (emotional and loss of time) since they had to contact their bank and replace their credit/debit card. This group is relatively large since TJX reported that approximately 75 percent of the credit cards stored in the breached files already expired or the associated PIN numbers were not stored in those files.[22]
3. Consumers who took advantage of the special discounts. Based on a sales report published by TJX, it appears that due to their extensive advertising campaigns and special discounts, the number of shoppers increased after the attack. TJX reported an 8 percent increase in revenue over the previous year.[23] Some of these shoppers may be considered winners in that they were able to take advantage of the breach to gain access to better pricing while not suffering losses due to the hacking.

Credit cards companies and issuers

Financial transactions especially ones involving credit and debit cards encompass several stakeholders. Each of these entities was impacted to some extent by the breach.

1. The most injured and the most vocal group in this case were the banks, the credit unions, and other credit issuing entities. These companies incurred two major expenses.
   a. Banks and credit unions that reissued a large number of cards. For example, Bank of Vermont reissued 1,600 cards.[24] The cost to replace a card is approximately $100. HarborOne Credit Union sent TJX a bill for $590,000, of which $90,000 was the cost to replace 9,000 credit cards and $500,000 for "brand damage."[25]
   b. Card issuers often are responsible for bogus charges. When a stolen credit card number was used, the issuer has to cover the losses. As of January 2008, there are no reports detailing the total amount lost by card issuers. While HarborOne chose to submit a bill to TJX, most other credit cards issuers chose legal recourse. For example, the Massachusetts Bankers Association and the Maine Association of Community Banks filed class-action lawsuits against TJX in a Massachusetts court.[26] Some banks also suffered brand name damage. For example, Fidelity Homestead was the first bank to discover that some of their customers suffered identity theft. This discovery was made prior to the TJX announcement. It was assumed that the hackers obtained the card numbers from the bank itself.[27] Fidelity Homestead estimated their loss from the breach at $23,000. Similarly, Fifth Third Bancorp was named in a California suit.[28]
2. Credit card companies such as Visa, MasterCard, and American Express attempt to impose certain standards to ensure the security of financial transactions. Because these standards are not government regulations, there is no legal recourse for noncompliance. The most widely known standard for using credit cards is the PCI/DSS standard. The cost of compliance is difficult to calculate since Payment Card Industry (PCI)/Data Security Standard (DSS) is a moving target—its requirements change as technology changes and hackers' sophistication increases.[29] Surveys conducted by credit card

[21] Although TJX did not publish a number, it is known that the Florida gang used credit cards to purchase $400 gift cards totaling $8M. One can conclude that the Florida gang bought approximately 20,000 cards. In addition, anecdotal data reported other cases where thousands of cardholders around the world were affected.

[22] Although not having an immediate access to the PIN number may create some difficulties, a reasonably good hacker can break a four-digit PIN number in less than a minute. Therefore, not having the associated PIN number is somewhat irrelevant for most hackers.

[23] http://www.eweek.com/c/a/Retail/The-Meaning-Of-TJXs-168-Million-Data-Breach-Cost/

[24] http://www.windowsecurity.com/articles/hackable-website-security.html

[25] http://www.computerworlduk.com/management/security/cybercrime/news/index.cfm?newsid=3372

[26] https://www.massbankers.org/pdfs/DataBreachSuitNR5.pdf

[27] http://money.cnn.com/2007/09/21/news/companies/bc.apfn.tjx.settlement.ap/index.htm

[28] http://money.cnn.com/2007/09/21/news/companies/bc.apfn.tjx.settlement.ap/index.htm

[29] http://www2.csoonline.com/exclusives/column.html?CID=33432

companies show that only 35 percent of large merchants (processing more than six million credit card transactions a year) are fully compliant, while 51 percent filed a document stating they intend to comply. Fourteen percent of large merchants did neither.[30] Medium- to small-size merchants comply even less. The compliance rate among level 2 merchants (merchants processing between one to six million transactions a year) is 26 percent. Twenty-two percent filed an ROC, leaving 52 percent as noncompliant. Level 3 retailers (processing 20,000 to a million transactions annually) are more compliant—51 percent are fully compliant and 16 percent filed for ROC. As of September 30, 2007, Visa began imposing monetary penalties for noncompliance and providing incentives (via reduced exchange fees) to compliant merchants.[31] However, the penalties often are imposed on the processors who supposedly ensure the merchant's compliance. Many merchants claim that the standards are too complicated and need to be eased. Merchants also complain that paying the penalties is cheaper than implementing all of the technology and procedures required by the standard. Since Visa does not provide a list of compliant merchants, consumers are unable to influence merchants by shopping in compliant stores and avoiding more risky noncompliant stores. Furthermore, it is doubtful that with only a few credit card companies and with possible risk to their credit ratings, many consumers would go as far as to give up their credit cards (which risks reduced credit ratings), thus limiting the overall risk to the credit card companies.

3. Credit clearing houses/processors. Credit card transactions often go through a third-party vendor that checks the availability of funds and approves or rejects the transaction. Clearinghouses and processors are not necessarily affiliated with the issuing company or with the credit card company. They maintain a large amount of private information and also are expected to comply with PCI/DSS standards. Credit card companies cannot levy fines against merchants directly. Therefore, if there is a breach of privacy, companies like Visa usually fine the financial entity that processed the transactions. In the case of TJX, Fifth Third Bancorp was fined $880,000 by Visa.[32] The rationale behind the fines is that Fifth Third Bancorp should have known that TJX's systems were not up to standard and that they should have acted upon it. As of January 2008, it is unclear if TJX will compensate Fifth Third Bancorp for the fines. The ability of the processor to recover such damages depends on their contractual agreement with the merchant.
4. Point-of-sale equipment vendors and related service providers. See discussion below.

Figure 2 describes the relationships and financial damages accrued by these entities. Although TJX is the source of the breach, a majority of the burden is carried by the consumers (mostly punitive) and issuing banks (mostly financial). Similarly, credit cards companies set privacy-related standards, which companies are suppose to follow. However, the fines are often imposed on the processors rather than the merchants. The above analysis suggests that there is a disconnect between the entities that controls the data and the entities that are likely to suffer damages if the data is compromised.

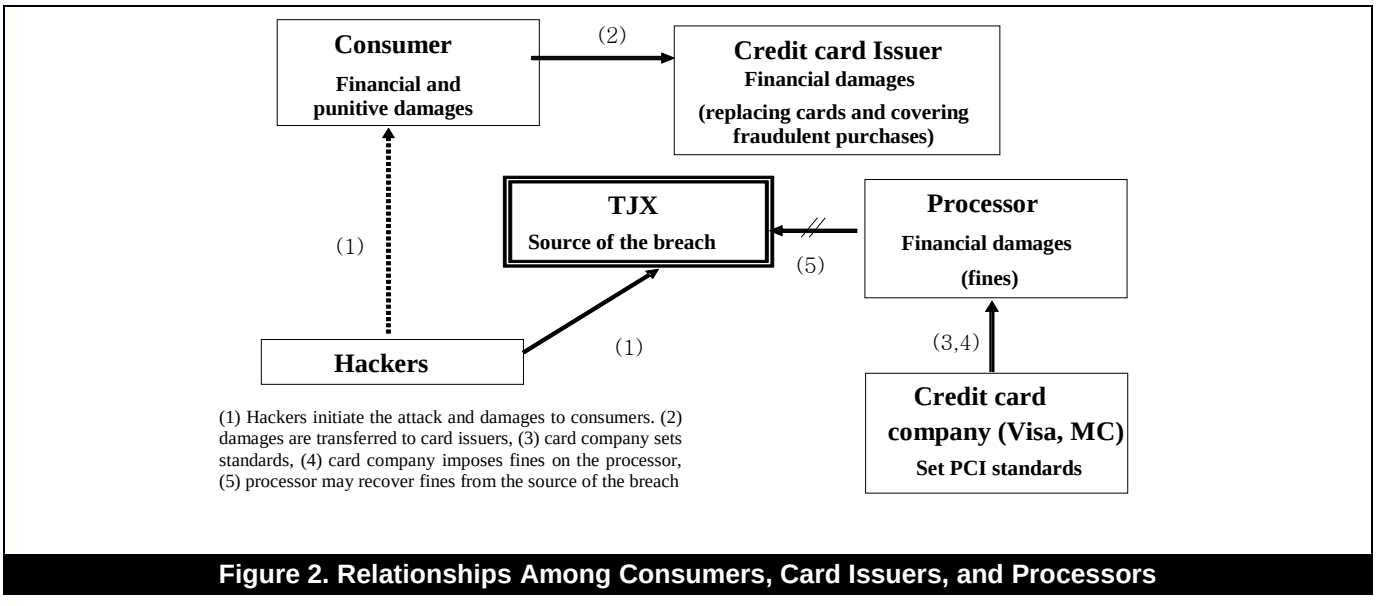

Figure 2. Relationships Among Consumers, Card Issuers, and Processors

[30] http://storefrontbacktalk.com/story/051007pci.php
[31] http://storefrontbacktalk.com/story/051007pci.php
[32] http://www.boston.com/business/globe/articles/2007/11/24/visa_fines_ohio_bank_in_tjx_data_breach/

Competitors

Yahoo! Finance (finance.yahoo.com) lists the following companies as TJX direct competitors: Kohl, Macy's, and Target. Although they are smaller in scope and were not included in the Yahoo! Finance list, we added Ross Stores Inc., since they have a similar business model to TJX. Table 2 (created January 26, 2008) compares TJX financials with its competitors.

Table 2: TJX Competitors

	TJX	Kohl's	Macy's	Target	Ross
Market Cap	13.21B	13.12B	10.80B	42.87B	3.58B
Employees	125,000	23,000	188,000	352,000	13,300
Qtrly Rev Growth	5.90%	4.80%	0.30%	9.30%	7.80%
Revenue	18.26B	16.38B	26.88B	63.21B	1.43B
Gross Margin	24.08%	36.87%	40.23%	32.74%	36.20%
Net Income	713.85M	1.16B	919.00M	2.94B	55.79M

The following are the stock symbols (tickers) of TJX main competitors: Kohl's = KSS, Macy's = M, Ross Stores = ROST, Target = TGT

The impact of the breach on TJX's competitors depends on their customers' reaction and behavior after the incident. TJX customers might react in one of several ways:

1. Abandon shopping at TJX stores such as TJ Maxx and Marshall, and shop at competitors such as Ross stores.
2. Continue to shop at TJX stores, but use more cash and less credit/debit cards.
3. Feel that all retailers are equally unsafe and reduce their shopping in all stores.
4. Resort to cash purchases not only at TJX stores, but at all stores. This might result in lower spending, since customers tend to spend more when they use credit cards [Feinberg, 1986].

The first reaction is beneficial to TJX competitors, since it will increase their customer base. Reaction 2 will have minimal affect on TJX's competitors. Reactions 3 and 4 will have a negative impact on competitors. Ettredge and Richardson [2001] showed that unexpected calamity to a given company can cause a negative spill-over effect, where competitors suffer negative market reaction to such an event.

Suppliers and other providers

TJX traditionally buys remainder merchandise from various Department Stores.[33] A major reduction in sales is likely to affect TJX's entire supply chain, causing it to buy fewer products, use less transportation, warehousing, and other logistics services, and potentially close-up stores and reduce their workforce. However, the security breach did not result in a reduction in sales. On the contrary, according to TJX's press release dated January 10, 2008, sales reports showed an unexpected increase. TJX holiday sales (five weeks ending January 5, 2008) were up by 6 percent from 2006/7 and their forty-eight weeks ending January 5, 2008, were up by 7 percent over the previous year.[34] In January 2007, TJX closed thirty-four A.J. Wright stores. However, the closure was planned before the intrusion was public and was unrelated to the breach.[35] TJX leases a majority of their real estate used for their stores and distribution centers. A major decrease in business could have affected their lessors. However, in 2007, TJX increased the total square footage it leases. Thus, the impact of the breach on the TJX supply chain appears positive.

Employees

The impact of the attack on TJX employment was minimal. TJX did not close any stores after the attack, nor did they institute major lay-offs. On the contrary, according to the TJX SEC filling from March 28, 2007, TJX increased the number of its stores by 4 percent. In addition, the attack was not the result of a social engineering scheme. Therefore, no new employee policies, training, or usage agreements were necessary, and none of the employees was held responsible. It is possible that some employees were asked about the attack and the safety of using credit

[33] According to TJX filing, the company is an opportunistic buyer. That is TJX buyers look for "deals" rather than have long-term contracts with one or two suppliers.

[34] http://www.businesswire.com/portal/site/tjx/index.jsp?epi-content=GENERIC&newsId=20080110005527&ndmHsc=v2*A938775600000*B1202282444000*C4102491599000*DgroupByDate*J2*N1001148&newsLang=en&beanID=1809476786&viewID=news_view

[35] http://google.brand.edgar-online.com/EFX_dll/EDGARpro.dll?FetchFilingHTML1?SessionID=C_VYWOA2hwhr7Nh&ID=5534546

cards at TJX stores. However, a search of the blogs covering or commenting on the attack did not record an outbreak of animosity toward TJX employees.

TJX management team[36]

As of January 27 2008, the president and CEO of TJX, Carol Meyrowitz owned 335,710 shares, as reported on 02/2008. Ms. Meyrowitz was not the CEO at the time of the security breach and was appointed a CEO in January 2007. The prior CEO, Bernard Cammarata, who owns 1,052,500 shares,[37] remained the chairperson of the Board. Only one executive exercised his options for 13,800 stocks (buying at an option price of $19.85 per share and selling at a market price of $31.85 per share for a gain of approximately $165,000) shortly after the breach was announced. However, in September 2006, three months before the discovery of the breach, almost every TJX officer exercised some of their options. Since TJX stocks were not performing any worse than the rest of the market, selling these stocks would not have benefited the executive team in comparison to liquidating other equities.

Information Technology vendors and auditors

Although most experts agreed that the intruders were able to access the system via the wireless connection between a store's point-of-sale equipment and their Retail Transaction Switch (RTS), very little has been written about the solution provider, vendors of point-of-sale equipment, and the vendors role in the breach. A rare reference to the technology used by TJX is found in the March 26, 2007, SEC filing:

> *We rely on commercially available systems, software, tools and monitoring to provide security for processing, transmission and storage of confidential customer information, such as payment card and personal information. We believe that the Intruder had access to the decryption algorithm for the encryption software we utilize. Further, the systems currently used for transmission and approval of payment card transactions, and the technology utilized in payment cards themselves, all of which can put payment card data at risk, are determined and controlled by the payment card industry, not by us*.

A press release dated January 2003 from Triversity Inc. states that TJX selected their product as its corporate-wide software platform for all their point-of-sale needs.[38] In September 2005, Triversity was bought by System Analysis and Program Development (SAP). Fujitsu Transaction Solutions Inc. is a solution provider in the retail industry; it services most of the large retailers, including TJX Inc.[39] In January 2006, Fujitsu Transaction Solutions Inc. partnered with AJB Software, a vendor that provides RTS and other payment solutions for the retail industry.[40] AJB also provides merchants with point-of-sale solutions. It is unclear if AJB products were implemented in any of the TJX stores. Nor is it clear what role Fujitsu Transaction Solutions Inc. had in the implementation of the initial solution and the upgrading of the wireless encryption from WEP to WPA. However, since TJX is now required to upgrade their system, it is likely that the vendors discussed here or their competitors will gain additional work.[41] After the breach, TJX hired a team of fifty security experts to investigate the breach and help correct their security measures.[42] In addition, as stated previously, TJX hired IBM and General Dynamics Corp. to help investigate the attack and upgrade their systems. The initial cost to investigate the breach and clean TJX systems was approximately $5 million. Although little is written about the above vendors, it appears that IT vendors and auditors realize financial gains after such an attack. The same vendors charged with securing a system are also charged with investigating and resolving attacks against that same system. This paradox has not been discussed in the literature.

Television/Radio stations and advertising agencies

Following the information security attack, TJX launched a massive advertising campaign.[43] This campaign included television, radio, and newspaper advertisements. TJX reported a 20 percent increase in advertising expenses. The company's advertising costs for 2007 are estimated at $244.7 million compared with $203 million for 2006 and $185 million for 2005.[44] Although officially TJX has not used the security breach as the reason for the increase, the $40 million boost in advertising budget benefited the advertisement and broadcasting industries.

---

[36] http://www.tjx.com/corprespons/corpgov_board.html
[37] http://finance.yahoo.com/q/mh?s=TJX
[38] 2003 is the reported time when TJX began installing its current Wi-Fi based POS system. In addition, some reports indicate that TJX had some problems with the initial installation and, therefore, retained customers' data longer than necessary (based on the Canadian PCC report).
[39] http://www.ajbsoftware.com/news.aspx?menuId=10901&id=61
[40] http://www.ajbsoftware.com/home.aspx
[41] There were no announcements of TJX replacing their solutions providers or that TJX is placing any responsibility of their vendors.
[42] http://online.wsj.com/article_email/article_print/SB117824446226991797-lMyQjAxMDE3NzA4NDIwNDQ0Wj.html
[43] http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1241259,00.html
[44] Based on the TJX 10K filing

Lawyers

Seth C. Harrington Ropes & Gray LLP, (BOS) One International Place Boston, MA, is the firm listed as representing TJX in the various lawsuits filed in the United States District Court, District of Massachusetts, as indicated in a district report dated October 12, 2007.[45] A number of other law firms represent the plaintiffs. Regardless of the outcome and the payment arrangements, these firms are winners. Either they receive large retainers or they enjoy potential future rents due to publicity.

Federal and state government

Investigators

Immediately after the intrusion was detected, federal agencies began investigating the information security attack. The investigation involved a number of agencies such as the secret service, Federal Bureau of Investigation (FBI), and local police authorities. As of January 2008, TJX was being investigated by Attorney Generals from roughly thirty states (led by Massachusetts)[46] and the Federal Trade Commissioner (FTC). These investigations are time- and resource-consuming and require the investment of taxpayers' funds.

Judicial system

Lawsuits increase the load on the judicial system, particularly in the District Court of Massachusetts. Overall, a major attack such as the TJX case creates financial and scheduling strains on the federal and state judicial system. If TJX was found guilty, it might have been required to pay fines that would have covered some of the expenses. However, as stated later in the case, TJX was not found to be liable for the attack, and thus these losses have not been recovered.

Legislation

As of January 2008, legislation had not been passed that forces retailers to correct vulnerabilities. Some states implemented laws that compel companies to inform customers of any vulnerabilities or breach of privacy (e.g., CA SB-138 in California), but current laws do not penalize merchants for not repairing their systems.[47] Similarly, compliance with PCI/DSS (see discussion above) requires the approval of a certified security assessor (also known as an *ASV*). However, ASVs are not regulated and do not suffer repercussions if they certify a vulnerable merchant. Furthermore, a cyber security bill proposed in California that would have imposed penalties on vulnerable companies was vetoed in October 2007.

Innocent bystanders

In addition to the above stakeholders, a breach (much like other crimes) can impact innocent bystanders that have no relation to the attacked company or the intruders. While in physical crime the reach is within a geographical proximity (such as a drive-by shooting), in cyber crime the reach is undetermined. In the case of TJX, one such party was Wal-Mart. In November 2006, a month before TJX discovered the security breach and two months before the public announcement, a Wal-Mart employee's vigilance unearthed $8 Million in fraudulent purchases. The criminals used credit card numbers from the TJX breach to purchase gift cards at Wal-Mart. The gift cards were then used to buy merchandise at Wal-Mart and Sam's Club stores all over Florida for a period of seventeen months. While a fraudulent credit card purchase can create an alert within a few hours (i.e., the card is canceled), a gift card takes months to track down, giving hackers a longer window of opportunity to exercise their option. It was only in January 2007 that law enforcement agencies realized that the TJX and Wal-Mart cases were connected.

[45] http://pacer.mad.uscourts.gov/dc/cgi-bin/recentops.pl?filename=young/pdf/tjx-07-10162-memorandum%20and%20order.pdf
[46] http://www.eweek.com/c/a/Security/Massachusetts-Leads-National-TJX-Data-Probe/
[47] http://www.eweek.com/c/a/Security/Security-Experts-Merchants-Racing-to-the-Bottom-for-PCI-Certs/1/

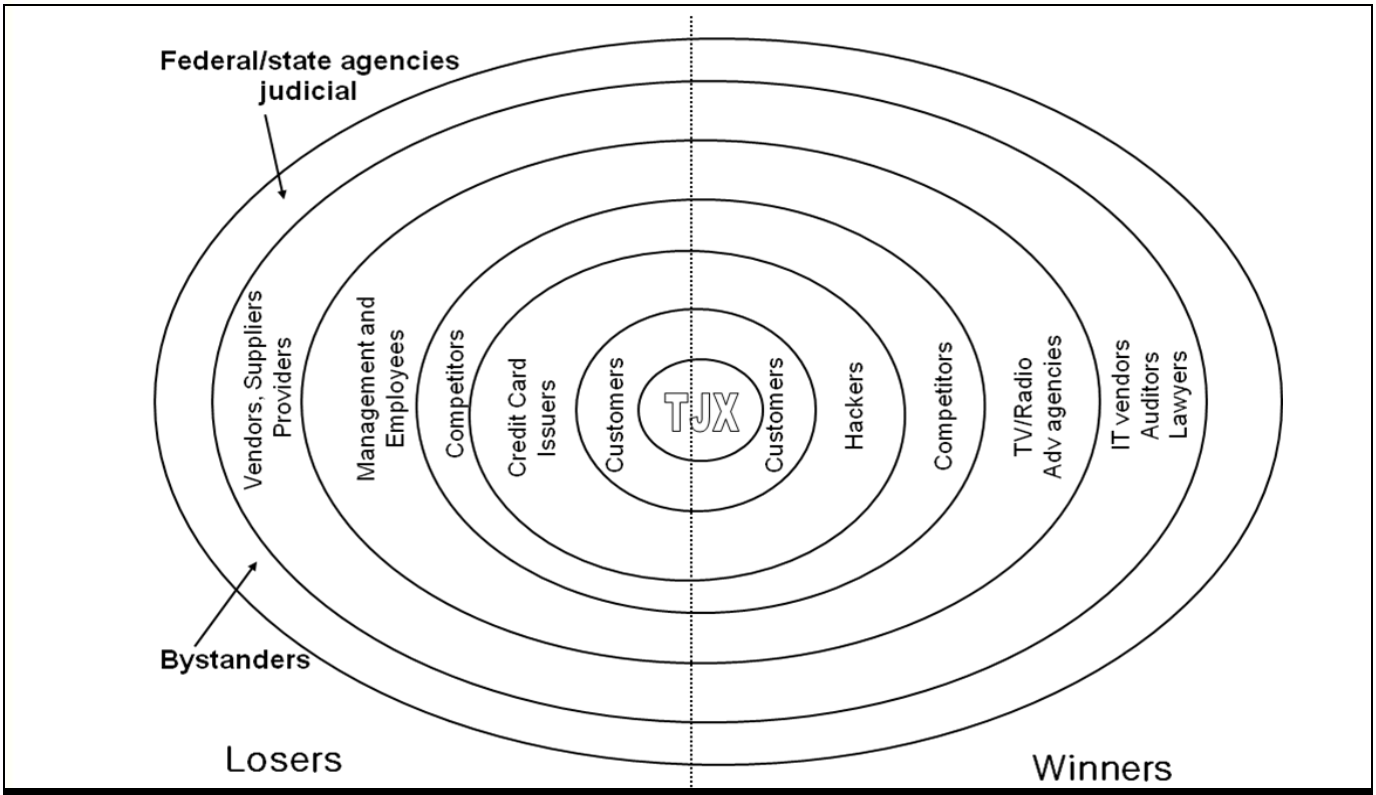

Figure 3. Winners and Losers in the TJX Case

How Was Each Stakeholder Affected?

As shown in Figure 3, some stakeholders are classified as winners and some as losers. However, some stakeholders such as TJX and their customers can be considered losers and winners. Figure 3 illustrates the far-reaching ripple effect of a security breach, much like a pebble thrown into a pond.

V. TJX MARKET POSITION AND FINANCIAL VITALS

To quantify TJX perceived risk, we look at the market value of TJX over time. The perceived risk analysis begins January 2007 when the public was first notified of the security breach and ends April 2008 when TJX settled with Master Card. A company's stock value represents the stock market's assessment of actual performance, reported losses and investors' confidence in the future of the company (e.g., trust, brand name, customers loyalty). On January 17, 2007, TJX stock value decreased slightly. However, by the next day the stock regained its value to a 1 percent increase over the Standard and Poor's (S&P) 500. According to finance.yahoo.com, as of March 28, 2008, TJX stock has outperformed its competitors. While the stock value of retailers such as Macy's and Kohl's suffered almost 40 percent loss, TJX stock increased by 20 percent in the twelve months following the attack. In addition, TJX stock value out-performed market averages (Figure 4).

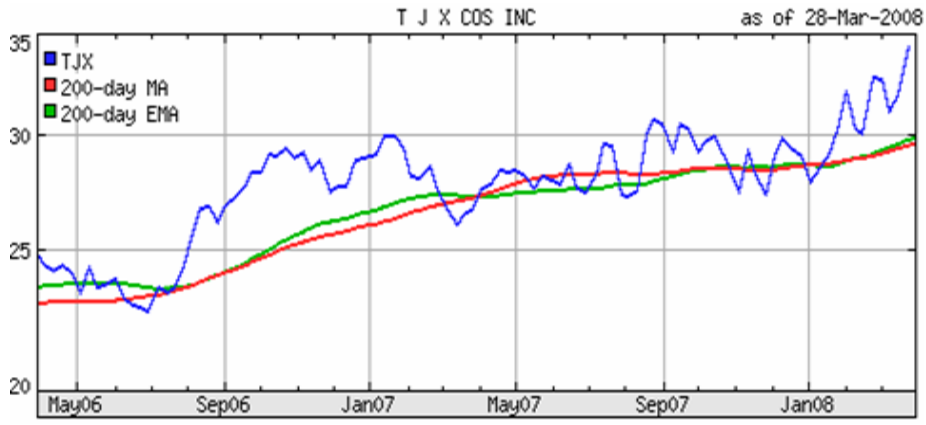

Figure 4. TJX Stock Performance vs. S&P500

In addition, TJX's Beta was 0.59 at a 2.44 percent change over the course of the year compared with the S&P 500 fifty-second-week change of -6.44.[48] Table 3 compares TJX financial vitals to their competitors. Some highlights of Table 3:

- Target's beta was higher at 1.2 and its stock value change for this year was -14.27 percent. This is more than twice as much as the S&P 500.
- Kohl's beta is calculated at 1.02. Kohl's stock fifty-two-week change is -39.32 percent.
- Macy's beta is 1.08. Macy's stock lost over 38 percent of their value during the same period.
- TJX management efficiency indicators (return on equity and return on assets) are much better than their competitors'.

Table 3: TJX Financial Vitals Compared to their Competitors

	TJX	TGT	KSS	M	ROST
Beta	0.59	1.2	1.02	1.08	0.45
Δ Stock value (52 wks.)	2.44%	-14.27%	-39.32%	-38%	-17.38%
ROA	10.75%	8.30%	11.58%	4.54%	11.78%
ROE	33.08%	18.99%	20.41%	8.16%	29.02
Q Earning Growth	8.20%	-4.50%	-13.60%	N/A	10.80%

TJX Risk over the Duration of the Event

To calculate the risk associated with the TJX information security attack over the duration of the event, we employ event study methodology. Event study methodology has been used in prior MIS research (e.g., Subramani and Walden, 2001; Im, Dow, and Grover, 2001; Dos Santos, Peffers, and Mauer, 1993) and in the assessment of cyber risk [Hovav and D'Arcy, 2003].

If an announcement contains information, it should cause the market to revalue the firm. Determining whether these announcements affect a firm's stock price requires that we estimate what the firm's stock price would have been had there been no announcement. To do this and to control for overall market effects, the return of the stock is regressed against the return of a market index. Details of the methodology and calculations used can be found in Hovav and D'Arcy [2003].

The market model was estimated for every major announcement related to the TJX security breach between January 17, 2007, and April 2, 2008 (see Table 1 for the TJX timeline). We used EVENTUS software to calculate abnormal returns and their associated p-value. Table 4 lists the events and the financial impact of each announcement on TJX market value.

Table 4: Financial Impact of TJX Announcements

Event Description	Abnormal Returns, (0.1)	Market adjusted z-test	p-value
Initial announcement	-0.69%	-0.517	N.S.
Attack larger than expected	-1.45%	-1.077	N.S.
Lawsuits by bank assoc.	-2.13%	-0.604	N.S.
Estimated attack cost $1.6B	-0.95%	-0.970	N.S.
Earning reports better than expected, estimated cost $118M	5.11%	3.983	0.001
Dismissal of class-action lawsuit	4.43%	3.527	0.001
TJX settles with Visa	3.67%	2.706	0.01
TJX settles with FTC	0.19%	0.951	N.S.
TJX settles with MC	0.84%	1.036	N.S.

For example, after the initial attack, the TJX abnormal return for the day of the attack was -0.69 percent and the standardized z-score was 0.517. Using Z-statistics, the TJX negative abnormal return for the day of the initial attack was not statistically significant. Similarly, TJX experienced negative abnormal returns after the following announcements: the actual size of the attack (over 45 million records), the slew of lawsuits specifically by the

[48] Analysis was conducted at the end of January 2008.

Massachusetts Banks Association, and the initial estimated cost to recover by industry analysts of $1.6 billion. However, none of the z-scores were statistically significant. It is important to note that during the first several months after the initial security breach announcement there were a large number of news articles regarding the attack. However, we chose to investigate the events that we felt were most severe and would have had the most impact. On August 14, 2007, TJX published their quarterly earnings report. The report included a cost and recovery assessment for the attack totaling $118 million. This assessment was substantially lower than prior calculated approximations and resulted in a positive abnormal return of 5.11 percent (p-value <0.01). Similar positive abnormal returns occurred after a judge dismissed several class-action lawsuits and when TJX settled with Visa. All three events resulted in statistically significant positive abnormal returns. The last two events resulted in positive returns. However, these returns were not statistically significant (see Figure 5).

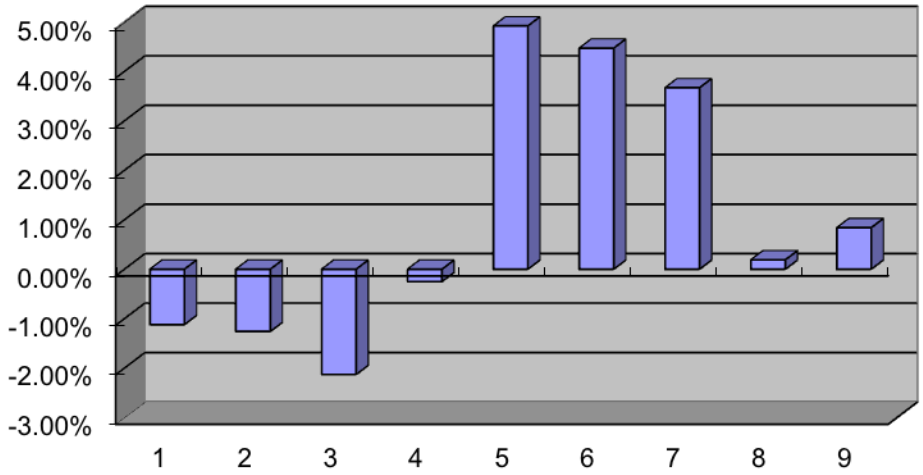

Figure 5. Abnormal Returns of TJX Stock

From the above data, one can conclude that, although the market reacts negatively to major security attacks, over time new information results in the market renewed interest. In the case of TJX, once the damage was assessed as substantially less than initially estimated, the positive reaction is significant. Similar reaction is observed when all class-action lawsuits are dismissed and when TJX settles with Visa. However, one can assume that a different type of news could have resulted in different market reaction.

VI. DISCUSSION

Stakeholder analysis enables us to examine in detail the affect of an information security incident on the various entities concerned with that attack and the ecosystem of the attacked company. Some stakeholders are losers and some are winners. Thus, the common assumption that all information security attacks result in overall financial losses to the entire economy should be further investigated. As is apparent from the above analysis, the main losers in the TJX case are some of the consumers (the ones whose credit card numbers were sold by the intruders), issuing entities (banks and credit unions), and credit processors (clearing house).

TJX itself appears to be both a loser and a winner. While TJX lost money and reputation, they have gained customers and sales. TJX financial vitals are superior to those of their competitors. Additionally, TJX stock has performed better than the market in the twelve months subsequent to the initial announcement. This appears counterintuitive since TJX had to pay out-of-pocket to investigate the attack and ratify their system and for legal expenses and settlement costs. Other losers include the judicial system and law enforcement agencies. The attack also resulted in a loss by Wal-Mart who is an innocent bystander with inconsequential relations to TJX.

The rest of the entities in the TJX ecosystem are winners, including some of the consumers who enjoyed additional discounts without being directly affected by the security attack. In addition, the TJX legal team, IT vendors, auditors, and advertising agencies all gained from the attack.

It is our contention that, since there are no regulations that require retailers to maintain a certain level of privacy (unlike the healthcare industry and HIPAA), companies might have minimal incentives to invest in information security. Although credit card companies attempt to impose standards via fines, the level of compliance is low and the fines are indirect.

The TJX case study is a first step in trying to understand the risk of a security attack beyond the scope of one company. The initial estimated potential cost of almost $2 billion was considered detrimental, and some analysts believed that TJX will be unable to withstand the tangible and intangible costs of the attack. Over time, more realistic cost estimates and the dismissal (or out of court settlements) of all relevant lawsuits were viewed by the market as "good" news resulting in increased market value for TJX. Therefore, rather than reacting immediately to major information security attacks, it might be prudent for investors to adopt a "wait and see" approach.

VII. CONCLUSIONS AND FUTURE RESEARCH

As a case study, the above analysis is not generalizable beyond the scope of the studied company. The case analysis used secondary data and publically available documents and news stories. Future research can benefit from access to actual firms' financials and interviews with executives after a major security incident. In addition, the study focused on the retail industry. Other industries may react differently. Future research could examine the ripple effect of an attack throughout the ecosystem of companies in various industries.

The analysis indicates that over time TJX was not a loser. On the contrary, the company gained customers and market share and was able to settle with various stakeholders (i.e., Visa and Master Card) for less than initially anticipated. In addition, all the class-action lawsuits were dismissed. Thus, it appears that TJX suffered negligible financial losses over time (if any) and had minimal legal repercussions. The TJX case highlights a notable challenge related to information security; the interplay among control, accountability, and liability. While TJX had full control over the compromised data, it was not held fully liable for the breach or accountable for a majority of the damages (also see Figure 2). This analysis implies that, without legislative and regulatory frameworks, companies have no real incentives to invest in organizational security countermeasures. However, due to the fluid nature of cyber attacks, these regulations or policies need to be universal.

The above issue manifests itself in another dimension—the accountability and liability of cyber criminals. The TJX intruders were from a variety of countries. While a few were arrested and brought to justice, others remain at large. The existence of "safe havens" for cyber criminals and the ability to perform cyber attacks remotely create a prosecutorial void. That is, it is very difficult to arrest and prosecute cyber criminals if and when they operate from "safe havens." Ideally, global measures need to be established and enforced to ensure the future development of a digital society. Without such measures, advances such as the "Internet of things" and pervasive computing might be perceived as too risky to implement.

At present, there is very limited detailed, quantitative data about information security incidents. Although a few organizations collect cyber attack related data (i.e., CERT), the scope and depth is limited. There is a need to establish a global database incorporating detailed financial, procedural, and technical information about various cyber incidents. The database should be accessible to think tanks and researchers around the world. Given such a database, researchers can use "big data" and analytics to investigate the global effect of cyber attacks on various stakeholders, industries, and countries.

Furthermore, technology in general and security technology in particular change very rapidly. To maintain a "reasonable level of security,"[49] companies have to upgrade their systems continuously. These upgrades are costly and disruptive. The TJX attack occurred while TJX was in the process of gradually upgrading their wireless encryption. Had TJX upgraded all 2,500 stores at once, the attack may have been thwarted. Presently there are few "best-practices" based on past data and a limited set of definite standards for companies to follow. Without an established baseline, it is very difficult for managers to decide when and how to upgrade their information security wares or justify the expense.

TJX post-attack increased revenue and sales is counterintuitive. It is possible that TJX benefited from several actions they took after the initial announcement, such as replacing the company's CEO, engaging in advertising and marketing campaigns, and offering sales and coupons. Further research is necessary to understand consumers' behavior post-attack. For example, do consumers blame companies for such attacks? When are companies perceived as negligent and when are they perceived as victims? What actions or factors can change stakeholders' perceptions? Are these perceptions industry, country, or culturally dependent?

In summary, the above case is the first (and to the best of our knowledge the only) study to follow a major security attack from start to end. The longitudinal analysis highlights two additional findings. The initial announcement often contains only partial information. Over time, new information is discovered that will cause the market to react differently. Thus, investors might consider a "wait and see" approach to information security attacks rather than react

[49] We do not define "reasonable level of security," since the concept itself is complex and may vary by industry or country.

immediately. Despite media and popular press assertion that security attacks can collapse our financial markets and create havoc, thus far no academic study has been able to empirically prove that assertion. Over time, an attack produces some winners and some losers and may result overall in a positive or zero-sum to the attacked firm's eco-system.

ACKNOWLEDGMENTS

Paul and I followed the TJX case from the first announcement to its conclusion. We were at the final writing stage when Paul unexpectedly passed away on May 10, 2012. He was a mentor and a friend and will be greatly missed by all who knew him. This article is dedicated to his memory.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Anthony, J.H., C. Wooseok, and S. Grabski (2006) "Market Reaction to e-Commerce Impairments Evidenced by Website Outages", *International Journal of Accounting Information Systems*, (7), pp. 60–78.

Baginski, S.P., R.B. Corbett, and W.R. Ortega (1991) "Catastrophic Events and Retroactive Liability Insurance: The Case of the MGM Grand Fire", *Journal of Risk and Insurance*, (58)2, pp. 247–260.

Barber, B.M., and M.N. Darrough (1996) "Product Liability and Firm Value: The Experience of American and Japanese Automakers, 1973–1992", *Journal of Political Economy*, (104)5, pp. 1084–1099.

Bruning, E.R., and A.T. Kuzma (1989) "Airline Accidents and Stock Return Performance", *Logistics and Transportation Review*, (25)2, pp. 157–168.

Carroll, A.B. (1979) "A Three-dimensional Conceptual Model of Corporate Social Performance", *Academy of Management Review*, (4), pp. 497–505.

Carroll, A.B. (1999) "The Pyramid of Corporate Social Responsibility: Toward the Moral Management of Organizational Stakeholders", *Business Horizons*, (34), July/August, pp. 39–48.

Cavusoglu, H., B. Mishra, and S. Raghunathan (2004) "The Effect of Internet Security Breach Announcements on Shareholder Wealth: Capital Market Reactions for Breached Firms and Internet Security Developers", *International Journal of Electronic Commerce*, (9)1, pp. 69–104.

Cochran, P.L., and R.A. Wood (1985) "Corporate Social Responsibility and Financial Performance", *Academy of Management Journal*, (27)1, pp. 42–56.

Dranove, D., and C. Olsen (1994) "The Economic Side Effects of Dangerous Drug Announcements", *Journal of Law & Economics,* (37)2, pp. 323–348.

Dos Santos, B.L., K. Peffers, and D.C. Mauer (1993) "The Impact of Information Technology Investment Announcements on the Market Value of the Firm", *Information Systems Research,* (4)1, pp. 1–23.

Earp, J.B., A.I. Anton, L. Aiman-Smith, and W.H. Stufflebeam (2004) "Examining Internet Privacy Policies Within the Context of User Privacy Values", *IEEE Transactions on Engineering Management*, (52)2, pp. 227–237.

Etebari, A., J.O. Horrigan, J.L. Landwehr (1987) "To Be or Not to Be—Reaction of Stock Returns to Sudden Deaths of Corporate Chief Executive Officers", *Journal of Business Finance & Accounting*, (14)2, pp. 255–279.

Ettredge, M., and V.J. Richardson (2001) "Assessing the Risk in e-Commerce", Twenty-second International Conference on Information Systems, December 16–19, New Orleans, LA.

Feinberg, R.A. (1986) "Credit Cards as Spending Facilitating Stimuli: A Conditioning Interpretation", *Journal of Consumer Research*, (13)3, pp. 348–356.

Gallivan, M. (2001) "Meaning to Change: How Diverse Stakeholders Interpret Organisational Communication About Change Initiatives", *IEEE Transactions on Professional Communication,* (44)4, pp. 243–266.

Grimble, R., and K. Wellard (1997) "Stakeholder Methodologies in Natural Resource Management: A Review of Principles, Contexts, Experiences, and Opportunities", *Agricultural Systems*, (55)2, pp. 173–193.

Hoffer, G.E., S.W. Pruitt, and R.J. Reilly (1988) "The Impact of Product Recalls on the Wealth of Sellers: A Reexamination", *Journal of Political Economy*, (96)3, pp. 663–670.

Hovav, A., and J. D'Arcy (2003) "The Impact of Denial-of-Service Announcements on the Market Value of Firms", *Risk Management and Insurance Review*, (6)2, pp. 97–121.

Hovav, A., and J. D'Arcy (2004) "The Impact of Virus Attack Announcements on the Market Value of Firms", *Information Systems Security*, (13)3, pp. 32–40.

Hovav, A., F.K. Andoh-Baidoo, and G. Dhllion (2007) "Classification of Security Breaches and Their Impact on the Market Value of Firms", Sixth Annual Information Security Conference, April 10–11, Las Vegas, NV.

Im, K.S., K.E. Dow, and V. Grover (2001) "A Reexamination of IT Investment and the Market Value of the Firm: An Event Study Methodology", *Information Systems Research,* (12)1, pp. 103–117.

Jarrell, G., and S. Peltzman (1985) "The Impact of Product Recalls on the Wealth of Sellers", *Journal of Political Economy*, (93)3, pp. 512–536.

Jensen, M.C., and W.H. Meckling (1976) "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure", *Journal of Financial Economics*, (3), pp. 305–360.

Johns, T.M. (1995) "Corporate Social Responsibility Revisited, Redefined", *California Management Review*, Spring, pp. 59–67.

Laudon, K.C., and J.P. Laudon (2007) *Management Information Systems: Managing the Digital Firm*, *tenth edition*, Saddleback, NJ: Prentice Hall.

Martin, R.L. (2002) "The Virtue Matrix: Calculating the Return on Corporate Responsibility", *Harvard Business Review*, (80), March, pp. 5–11.

McWilliams, A., and D. Siegel (2001) "Corporate Social Responsibility and Financial Performance: Correlation or Misspecification?", *Strategic Management Journal*, (21), pp. 603–609.

Metzger, M.J. (2004) "Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce", *Journal of Computer-mediated Communication*, (4)9, http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2004.tb00292.x/full (current October 30, 2013).

Miyazaki, A.D., and A. Fernandez (2001) "Consumer Perceptions of Privacy and Security Risks for Online Shopping", *Journal of Consumer Affairs*, (35)1, pp. 27–44.

Orlitzky, M., F.L. Schmidt, and S.L. Rynes (2003) "Corporate Social and Financial Performance: A Meta-analysis", *Organization Studies*, (24)3, pp. 403–441.

Pan, G.S.C. (2005) "Information Systems Project Abandonment: A Stakeholder Analysis", *International Journal of Information Management*, (25), pp. 173–184.

Posnikoff, J.F. (1997) "Disinvestment from South Africa: They Did Well by Doing Good", *Contemporary Economic Policy*, (15), January, pp. 76–86.

Pruitt, S.W., and D.R. Peterson (1986) "Security Price Reactions Around Product Recall Announcements", *Journal of Financial Research*, (9)2, pp. 113–122.

Richardson, R. (2007) "CSI/FBI Computer Crime and Security Survey", http://gocsi.com/sites/default/files/uploads/2007_CSI_Survey_full-color_no%20marks.indd_.pdf (current October 30, 2013).

Russo, M.V., and P.A. Fouts (1997) "A Resource-based Perspective on Corporate Environmental Performance and Profitability", *Academy of Management Journal*, (40), pp. 534–559.

Salin, V., and N.H. Hooker (2001) "Stock Market Reaction to Food Recalls", *Review of Agricultural Economics,* (23)1, pp. 33–46.

Siomkos, G.J. (1992) "Conceptual and Methodological Propositions for Assessing Responses to Industrial Crises, *Review of Business*, (13)4, pp. 26–31.

Sprecher, R., and M. Pertl (1988) "Intra-industry Effects of the MGM Grand Fire, *Quarterly Journal of Business and Economics*, (27), pp. 96–16.

Stewart, K.A., and A.H. Segars (2002) "An Empirical Examination of the Concern for Information Privacy Instrument", *Information Systems Research*, (13)1, pp. 36–49.

Subramani, M., and E. Walden (2001) "The Impact of e-Commerce Announcements on the Market Value of Firms", *Information Systems Research*, (12)2, pp. 135–154.

Thomsen, M.R., and A.M. McKenzie (2001) "Market Incentives for Safe Foods: An Examination of Shareholder Losses from Meat and Poultry Recalls", *American Journal of Agricultural Economics*, (82)3, pp. 526–538.

Waddock, S., and S. Graves, (1997) "The Corporate Social Performance Financial Performance Link", *Strategic Management Journal*, (18), pp. 303–319.

APPENDIX A: EXAMPLES OF FINANCIAL IMPACT OF CATASTROPHIC EVENTS

Examples of financial impact of catastrophic events:

- MGM Grand fire [Baginski, Corbett, and Ortega, 1991; Sprecher and Pertl, 1988]
- Airline accidents [Bruning and Kuzma, 1989]
- Product recalls and defective products in various industries such as auto, pharmaceutical, and electronics [Jarrell and Peltzman, 1985; Pruitt and Peterson, 1986; Hoffer, Pruitt, and Reilly, 1988; Barber and Darrough, 1996; Thomsen and McKenzie, 2001],
- Unexpected death of a CEO [Etebari A., J.O. Horrigan, J.L. Landwehr, 1987]
- Environmental accidents such as a chemical spill [Siomkos, 1992]

The share price of the subject company remained depressed from a few days to several months. The market reaction is often the result of the following factors:

- The direct cost to recover (including repair, replace, and notify customers)
- Legal and settlement cost resulting from liability lawsuits [Jarrell and Peltzman, 1985; Dranove and Olsen, 1994; Barber and Darrough, 1996; Salin and Hooker, 2001; Thomsen and McKenzie, 2001]
- Loss of the firm's "brand name capital" and reputation [Jarrell and Peltzman, 1985; Pruitt and Peterson, 1986; Hoffer et al., 1988; Barber and Darrough, 1996; Thomsen and McKenzie, 2001]
- Loss of future sales [Pruitt and Peterson, 1986; Dranove and Olsen, 1994; Salin and Hooker, 2001]
- Loss of consumer trust [Jarrell and Peltzman, 1985]

Major catastrophic events often result in stringent regulations that increase costs to develop and approve new products and, thus, reduce profitability [Hoffer et al., 1988; Thomsen and McKenzie, 2001].

ABOUT THE AUTHORS

Anat Hovav is a professor at Korea University Business School in Seoul, South Korea. Her research interests include the socio-technical aspects of organizational information security, risk assessment, innovation management, and electronic scholarship. Anat Hovav has published in internationally refereed journals such as *Information Systems Research (ISR), Information & Management, Communications of the ACM, Journal of Business Ethics, Research Policy, Computers & Security, Information Systems Journal (ISJ), Information Systems Management (ISM), Communications of AIS (CAIS), Information Systems Frontiers,* and *Risk Management and Insurance Review*.

Paul Gray (1930–2012) was Professor Emeritus and Founding Chair of the School of Information Science at Claremont Graduate University. He was the Founding Editor of the *Communications of the Association for Information Systems* from 1998 to 2005. His recent interests in information systems included business intelligence, knowledge management, data warehousing, e-commerce, and futures research methodology. Professor Gray retired in May 2001 but continued to teach, research, consult, and curate the Paul Gray PC Museum at Claremont. He was awarded the LEO Award of the Association for Information Systems for lifetime achievement. He was inducted as a Fellow of the Association of Information Systems and as a Fellow of the Institute for Operations Research and the Management Sciences. He was the author of over 160 journal articles and the author/editor of sixteen academic books.

Communications of the Association for Information Systems

ISSN: 1529-3181

Communications of the Association for Information Systems