Communications of the Association for Information Systems

Volume 23 | Number 1 Article 31

11-1-2008

Security Breach: The Case of TJX Companies, Inc.

William Xu
Carleton University, wxu3@connect.carleton.ca

Gerald Grant
Carleton University

Hai Nguyen
Carleton University

Xianyi Dai
Carleton University

Recommended Citation

Xu, William; Grant, Gerald; Nguyen, Hai; and Dai, Xianyi (2008) "Security Breach: The Case of TJX Companies, Inc.," *Communications of the Association for Information Systems*: Vol. 23, Article 31.
Available at: http://aisel.aisnet.org/cais/vol23/iss1/31

Communications of the Association for Information Systems

CAIS

Security Breach: The Case of TJX Companies, Inc.

William Xu

Gerald Grant

Hai Nguyen

Xianyi Dai

Carleton University, Sprott School of Business

wxu3@connect.carleton.ca

Abstract:

TJX Companies Inc. is a leading off-price apparel and home fashions retailer with headquarters situated in the United States. In late 2006, the company discovered it was victim to a massive security breach which compromised millions of customer records. Despite the internal exchanges within the IT department concerning the upgrade of their wireless security standard protocol, the company opted for cost savings rather than increased spending. As the company financials took a hit, the company was faced with pending lawsuits from credit card companies and affected customers; government scrutiny of IT security standards; loss of consumer confidence; among other concerns. Though it has not yet concluded the extent of the financial impact of this incident, analysts estimate the full cost of the breach might amount up to one billion dollars. This case presents a "wake-up call" for retail companies about the importance of IT security.

Keywords: case study, information technology management, IT infrastructure, networking systems, organization, organizational unit, privacy, risk, security, teaching case

Volume 23, Article 31, pp. 575- 590, November 2008

The manuscript was received 10/13/2008 and was accepted on 11/5/2008.

I. INTRODUCTION

In early 2007, Carol Meyrowitz became CEO of TJX Companies Inc. Ranked among one of the 50 most powerful women in business, she went through many challenges in her career [Fortune Magazine 2007a]. Weeks prior to her promotion, it was discovered that hackers broke into the systems of TJX in late 2006 and stole vital customer information. This event proved to be one of the largest reported security data breaches to date, costing the company millions of dollars. Not only that, there was also a growing fear of customer distrust, government scrutiny, as well as lawsuits from credit card companies and contracting banks which may become critical to the company's core business. After the incident, former TJX group president Alexander Smith resigned. Gary Crittenden, CFO of American Express Co., also stepped down from TJX's board [Abelson 2007a]. The chairman, Bernard Cammarata; vice-chairman Donald Campbell; and public relations executive, Sherry Lang were among the few public figures who will work with Meyrowitz to guide TJX out of this public relations crisis (see Figure 1 for company organizational chart).

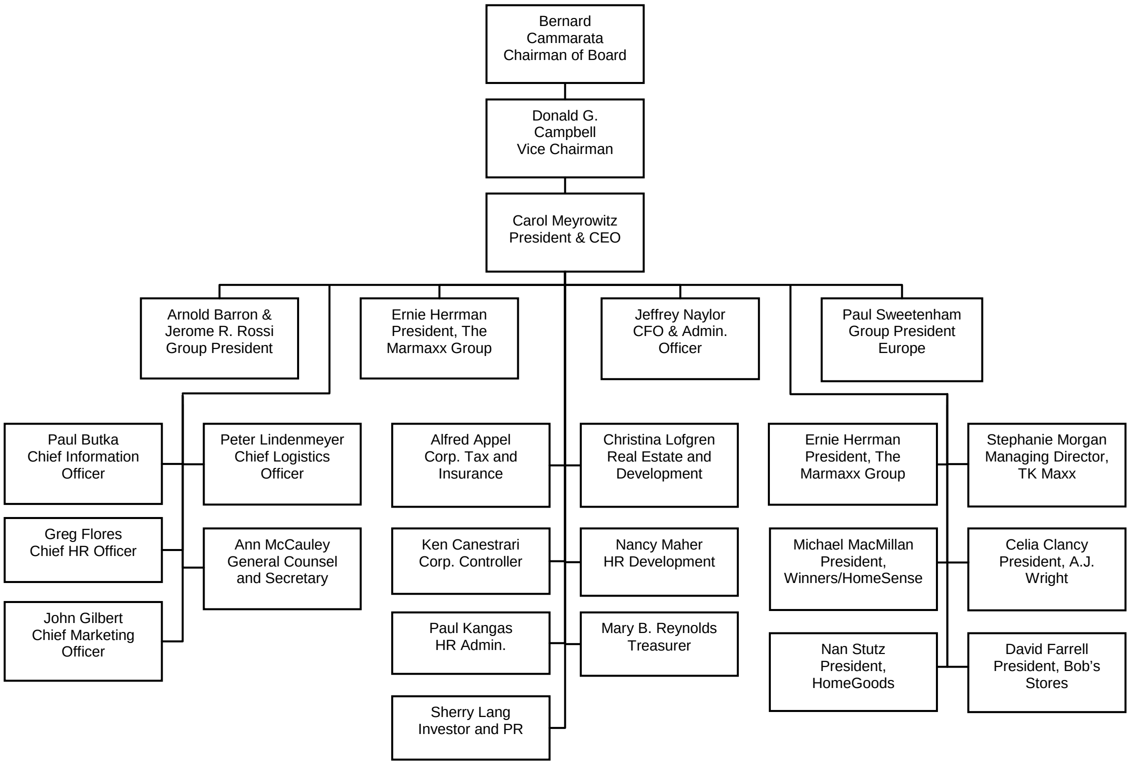

Bernard Cammarata Chairman of Board
Donald G. Campbell Vice Chairman
Carol Meyrowitz President & CEO
Arnold Barron & Jerome R. Rossi Group President
Ernie Herrman President, The Marmaxx Group
Jeffrey Naylor CFO & Admin. Officer
Paul Sweetenham Group President Europe
Paul Butka Chief Information Officer
Peter Lindenmeyer Chief Logistics Officer
Alfred Appel Corp. Tax and Insurance
Christina Lofgren Real Estate and Development
Ernie Herrman President, The Marmaxx Group
Stephanie Morgan Managing Director, TK Maxx
Greg Flores Chief HR Officer
Ann McCauley General Counsel and Secretary
Ken Canestrari Corp. Controller
Nancy Maher HR Development
Michael MacMillan President, Winners/HomeSense
Celia Clancy President, A.J. Wright
John Gilbert Chief Marketing Officer
Paul Kangas HR Admin.
Mary B. Reynolds Treasurer
Nan Stutz President, HomeGoods
David Farrell President, Bob's Stores
Sherry Lang Investor and PR

Figure 1. TJX Companies, Inc. Organizational Structure [The TJX Companies 2007]

II. COMPANY HISTORY: TJX COMPANIES, INC.

The TJX Companies, Inc. has a history of more than 50 years. Its origin can be traced to the discount department store named Zayre, which was founded in 1956 in Massachusetts, USA. In 1962, the Zayre store chain of discount department stores was incorporated as Zayre Corporation. In 1969, Zayre acquired the Hit or Miss chain and began its investment in the upscale off-price fashion market. The first branded-store, T.J. Maxx, opened in March 1977 in Auburn, Massachusetts [Funding Universe 2004]. By the first half of 1983, Hit or Miss and T.J. Maxx were producing nearly 45 percent of Zayre's income. Meanwhile, Zayre was renovating its chain of discount department stores and increasing its product line to suit its customers' needs. The number of Hit or Miss stores eventually rose to 420 in the United States by 1986. Sales for these latter department stores reached $300 million, a high figure in that sector at the time [Funding Universe 2004].

Establishment of TJX Companies and Its Expansion

In June 1987, under the leadership of president and CEO Bernard Cammarata, the TJX Companies, Inc. was established as a subsidiary of Zayre. But due to poor sales, Zayre suffered operating losses of $69 million on sales of $1.4 billion in the first half of 1988 while TJX continued to earn profit. This led to the decision to sell the entire chain of over 400 Zayre stores to Ames Department Stores, Inc. The following year, the company changed its name to The TJX Companies, Inc [Hoover's Company Records 2008a].

Throughout the 1990s, TJX expanded to Canada and Europe starting with the acquisition of the five-store Winners Apparel Ltd. chain in Canada. Several years later, the company ventured into the United Kingdom and launched T.K. Maxx in 1996. During that same time, the company leveraged the strong performance of its main chains by introducing experimental new hybrid formats as well as brand-new chains. In 1998, TJX opened two T.K. Maxx stores in The Netherlands as a preliminary step onto continental Europe.

TJX maintained its growth path into the 21st century. In spite of the poor economic environment of 2001 and the post-9/11 impact on the expenditure of consumers, the company still managed to increase revenues by 12 percent to $10.71 billion, breaking the $10 billion mark for the first time. In 2002, although faced with economic uncertainty, TJX once again managed to achieve a 12 percent jump in revenues. Eventually, all seven of the company's formats had expanded. In particular, the firm added 178 stores to the new total count of 1,843 stores [Funding Universe 2004]. A timeline of the company's history is presented in Appendix I.

Company Overview in 2006

In 2006, TJX Companies, Inc. was classified as the largest off-price apparel and home fashions retailer in both the United States and the world. Its main brand-stores are T.J. Maxx, Marshalls, Winners, HomeSense, HomeGoods, A.J. Wright, Bob's Stores, and T.K. Maxx. T.J. Maxx, the largest retailer of its kind in the United States, has 821 stores by 2006, offering brand-name family apparel, giftware, jewelry and accessories, home decor, and footwear. Marshalls, the nation's second largest off-price apparel retailer with 748 stores, includes the product line of T.J. Maxx but also has expanded footwear assortments [The TJX Companies 2007]. Venturing into Canada and the United Kingdom, the leading off-price family apparel chains were Winners and T.K. Maxx, respectively. In 1992, HomeGoods was introduced, operating 270 stores by 2006's year end. This branded-store offers giftware, accent furnishings, and seasonal merchandise. The majority of the firm's divisions target middle to upper-middle income consumers who are both value and fashion conscious. As the company's revenues reached $17 billion, the company ranked 133rd on the Fortune 500 list. By the end of the fiscal year 2006, TJX had 125,000 employees and over 2400 stores worldwide [Hoover's Company Records 2008a]. Appendix II shows further details of the company.

Industry and Its Major Competitors

In the United States, the off-price apparel retail industry is characterized as being relatively saturated with consumer buying power affecting the market. As a whole, in 2006, the industry grew 2.4 percent and generated total revenues of $295.5 billion. The majority of this revenue was attributed to the sale of women's apparel; accounting for more than 58 percent of the industry segment [Datamonitor 2007].

TJX's main competitors in the off-price apparel industry are Kohl's Corporation and Macy's Inc. As an American department store chain, Kohl's Corp. operates nearly 950 stores in 47 states. Based on 2006 revenues, the company was listed as 152 on the Fortune 500 list [Hoover's Company Records 2008b]. On the other hand, Macy's Inc., formerly known as Federated Department Stores, Inc., operates about 850 stores in the United States. Its 2006 revenues were $26.9 billion; greatly ahead of its immediate rivals [Hoover's Company Records 2008c]. Compared to its direct competitors, TJX's annual sales have been growing steadily from 1997 to 2006 (Figure 2).

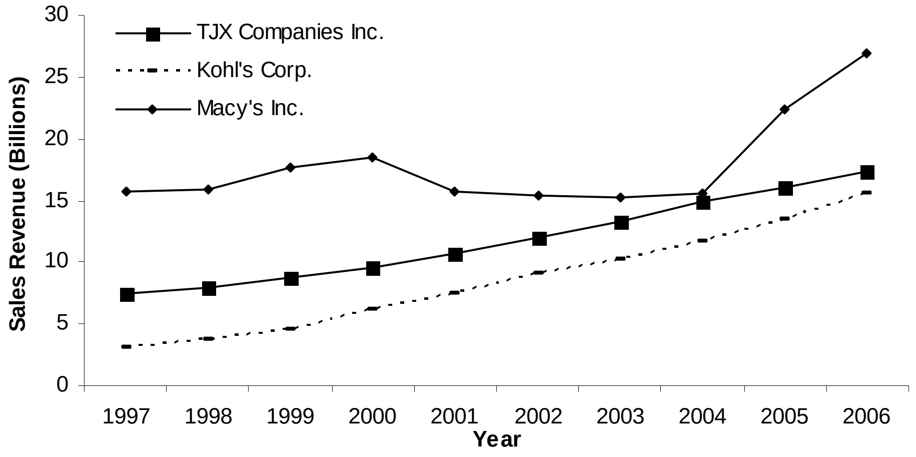


Figure 2. Annual Sales Revenue (1997-2006); TJX and Competitors [Mergent Online 2008]

III. THE E-COMMERCE EVOLUTION

As the emergence of the Internet in the mid-1990s opened many opportunities, retailers began taking advantage of this new innovation in conducting business. Electronic commerce (e-commerce) allowed the company to expand its marketplace nationally and internationally leading to activities by a company such as: easily and quickly locating more customers; enabling customers to shop or do other transactions 24 hours a day, all year round; the ability to organize and create highly specialized businesses; among other benefits [Hazari 2000]. Taken together, e-commerce allowed a reduction in overhead and inventories by facilitating a "pull-type" system where the process is initiated from the customer. More notably, as a tool to leverage the e-marketplace for its own competitive advantage, Amazon.com became one of the first examples to benefit from the e-commerce revolution. Retailers saw the potential to not only expand their storefronts, but as a way to create awareness of their business and products through this new channel [Turban et al. 2000].

Establishing a Web Presence

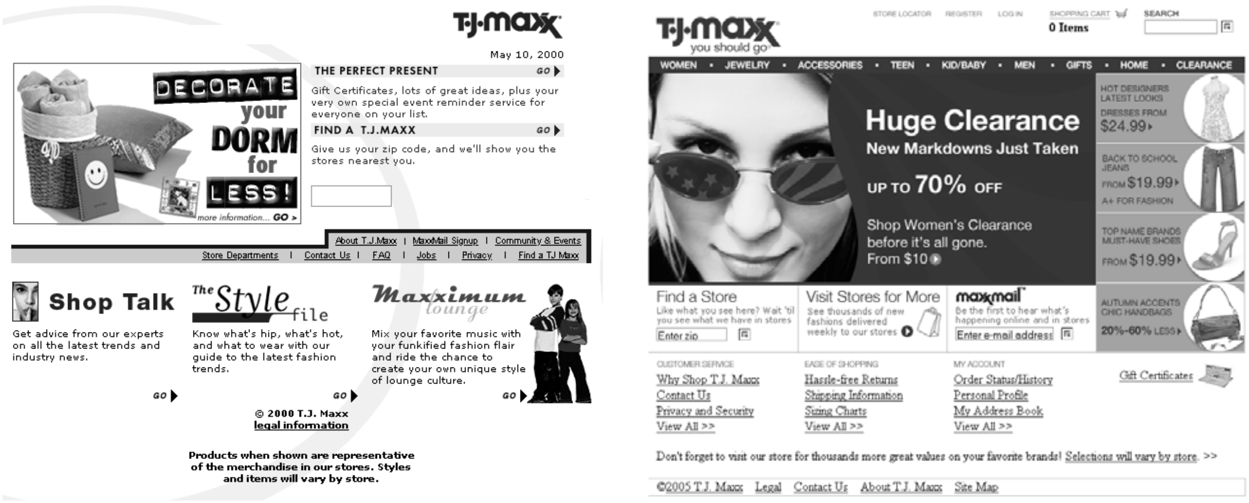
In November 1999, the company launched its first retail Web site for its popular T.J. Maxx branded-store. The various features included in its Web site were [Business Wire 1999]:

- *Store Locator* - customers were able to locate their nearest store; obtain driving directions
- *Style File* - a preliminary resource and information on holiday fashion trends and other tips
- *MaxxMail* - an e-mail newsletter for customers to keep them informed of community events and Web site updates

The Web site was mainly used as a means to provide customers' with up-to-date information about their store. Despite its use as a marketing-only channel, TJX soon realized that Internet traffic to the store Web site increased at a steady rate.

The Launch of the E-Commerce Web Site

Following the launch of its first Web site, the other stores followed suit. In 2004, as leading retail competitors such as Macy's have gained a significant online presence, TJX announced the launch of its first e-commerce web sites for two of its retail store brands; T.J. Maxx and HomeGoods. It was the first time the company offered its products for sale online (Figure 3 shows the transition).



May 10, 2000

Gift Certificates, lots of great ideas, plus your very own special event reminder service for everyone on your list.

Give us your zip code, and we'll show you the stores nearest you.

Get advice from our experts on all the latest trends and industry news.

Know what's hip, what's hot, and what to wear with our guide to the latest fashion trends.

Mix your favorite music with your funkified fashion flair and ride the chance to create your own unique style of lounge culture.

© 2000 T.J. Maxx

Products when shown are representative of the merchandise in our stores. Styles and items will vary by store.

TJMaxx.com (May, 2000)

0 Items

Shop Women's Clearance before it's all gone. From $10

Like what you see here? Wait 'til you see what we have in stores

See thousands of new fashions delivered weekly to our stores

Be the first to hear what's happening online and in stores

Don't forget to visit our store for thousands more great values on your favorite brands! Selections will vary by store. >>

©2005 T.J. Maxx

TJMaxx.com (May, 2005)

Figure 3. Establishment of E-Commerce Web Site [Internet Archive 2008]

Under the direction of president and CEO, at the time, Edmond J. English stated:

> *We see the Internet channel as a way to capture new T.J. Maxx and HomeGoods customers as well as offer our existing customers the convenience of shopping from home. We also see the Internet as a way to drive customer traffic to our stores, as we will market concepts and encourage customers to shop the wider selections offered in our stores.* [Business Wire 2004]

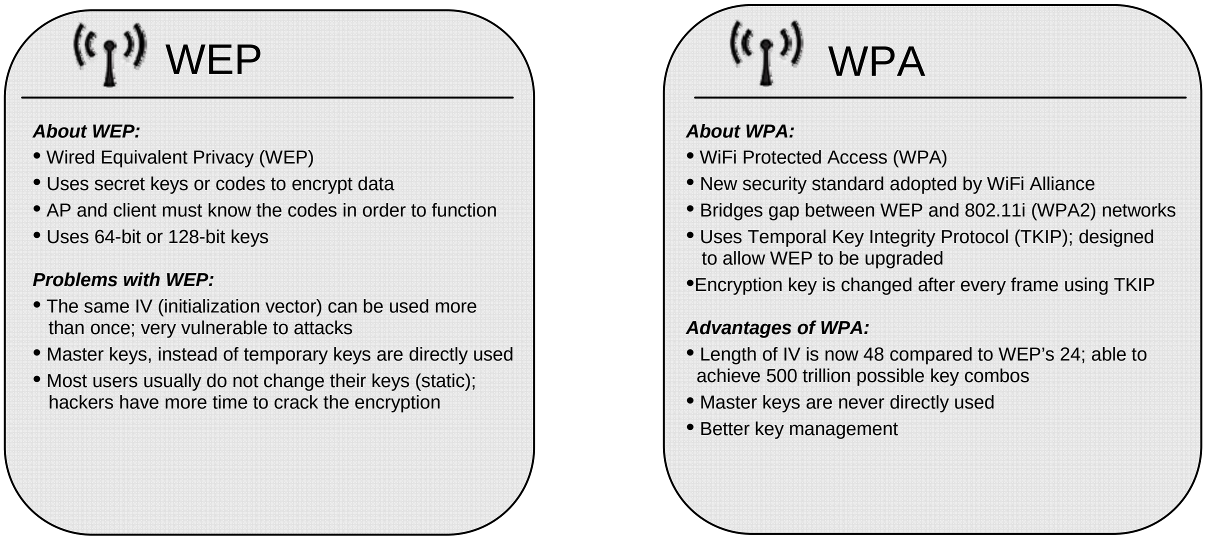
As demand and traffic to the original web site grew, Edmond knew this was the perfect opportunity for the two popular stores to expand their business strategy.

> *Having evaluated the Internet channel for several years, we believe it is the right time for TJX to enter e-commerce. We plan to operate these sites as extensions of our divisions, not as separate businesses, leading to lower operating costs and a clearer path to success. Further, we view e-commerce as a driver of incremental sales in the short term and a vehicle for significant growth over time.* [Business Wire 2004]

To offer customers more value; the company also decided to offer the chance for customers to return their merchandise purchased online to any retail store in the U.S. This added feature made notable by other brick-and-mortar extensions was becoming more significant.

IV. THE EMERGENCE OF WEP SECURITY STANDARD

When wireless first became a technology to be used, the industry realized that they needed a way to protect the information and data that was being transmitted. Wireless Equivalent Privacy (WEP) was an encryption code developed in 1999 that was built into all standard 802.11 wireless products. Using 64-bit or 128-bit keys, secret keys or codes to encrypt the data could be chosen by the client. However, by the year 2000, researchers and online hackers had discovered ways to crack the WEP encryption code in just seconds, leading to the development of a new emerging standard WiFi Protected Access (WPA) [Velte and Velte 2006]. Figure 4 compares the two wireless standards.



WEP

About WEP:

- Wired Equivalent Privacy (WEP)
- Uses secret keys or codes to encrypt data
- AP and client must know the codes in order to function
- Uses 64-bit or 128-bit keys

Problems with WEP:

- The same IV (initialization vector) can be used more than once; very vulnerable to attacks
- Master keys, instead of temporary keys are directly used
- Most users usually do not change their keys (static); hackers have more time to crack the encryption

WPA

About WPA:

- WiFi Protected Access (WPA)
- New security standard adopted by WiFi Alliance
- Bridges gap between WEP and 802.11i (WPA2) networks
- Uses Temporal Key Integrity Protocol (TKIP); designed to allow WEP to be upgraded
- Encryption key is changed after every frame using TKIP

Advantages of WPA:

- Length of IV is now 48 compared to WEP's 24; able to achieve 500 trillion possible key combos
- Master keys are never directly used
- Better key management

Figure 4. Wireless Security Comparison - WEP vs. WPA [Gerling 2006]

TJX adopted the use of the WEP security standard throughout its chain of stores. The use of wireless technology allowed TJX and other retailers to access data and information from retail-store servers as well as corporate servers. When product barcodes are scanned through their point-of-sale systems, wireless transmissions between the scan guns data receivers in-store and through corporate networks are established [Chickowski 2008]. Information is relayed instantly showing the current name and price of the item (Figure 5).

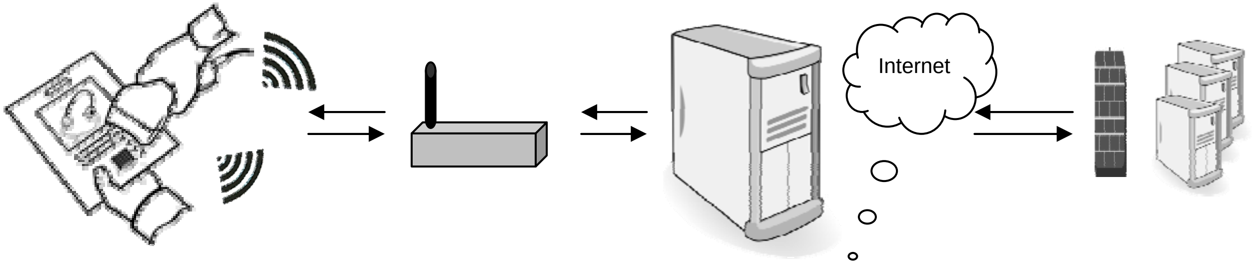


Figure 5. Wireless Transmission of Data Connected to Corporate Networks

Included in this wireless transmission of data is the ability for credit card companies to establish a connection to acquire customer credit card information from the retail store's computer system. TJX and other retailers were required by the credit card companies to store information about the customer's credit card on their own internal systems. The rationale for this was that in case of transaction disputes, a record of information can be accessed by the credit card company within the disputable time frame [The Associated Press 2008].

Payment Card Industry (PCI) Data Security Standard

In early 2004, the major credit card companies including Visa and MasterCard, decided to create additional means of protection for customers by enforcing security standards that merchants must meet. Retailers would need to comply with the storing, processing, and transmission of cardholder data through the updated guidelines enforced by the PCI standards council. Audits were required annually and for systems to be checked for external vulnerabilities by third-party auditors at least once a quarter [PCI Security 2006].

In December 2004, the first Payment Card Industry Data Security Standard (PCI DSS) was released (Appendix III shows the general requirements). It was mainly developed by the collection of credit card companies as a way to help organizations process credit card payments with the appropriate due diligence. This standard helped retailers reduce the risk of credit card fraud, cracking, and other security vulnerabilities and threats [PCI Security 2006]. However, the adoption of PCI DSS was not widespread, even though merchants can be fined for not complying. While there has been major progress updating security over the past few years, many companies still have not secured data for various reasons, some of them technical. For example, encrypting data on a mainframe is very difficult. Usually, the mistake that companies make is that they store the encryption key in the same database after the encryption process.

Because of the lack of full participation from retailers, the council recommended that every company, whether they are in the process of adopting PCI DSS or not, should make sure data is encrypted from the main data exchange and that the encryption key is secured in a safe manner. They further stated that there was "no point in having a database of encrypted credit card numbers if the key is in the same database" [Brodkin 2007].

The Wireless Security Investment Debate

Although the PCI policies were in place, TJX initially failed nine of the 12 requirements that were set; though, without any major penalties, Visa allowed TJX to resume normal operations on the condition that they would improve its security [Chickowski 2008]. At this same time, Chief Information Officer Paul Butka, knew that sales had picked up throughout the company and focused on a conservative approach to its internal security investments.

In an e-mail sent to his staff on November 23, 2005, Butka expressed his attitude towards the increased security compliance measures. He suggested delaying the upgrade of in-store wireless encryption standards from its WEP to the new emerging and more secure WPA standard. He wrote:

> *We can be PCI-compliant without the planned FY '07 upgrade to WPA technology for encryption because most of our stores do not have WPA capability without some changes…WPA is clearly best practice and may ultimately become a requirement for PCI compliance sometime in the future. I think we have an opportunity to defer some spending from FY '07's budget by removing the money from the WPA upgrade, but I would want us all to agree that the risks are small or negligible.* [Chickowski 2008, p.29]
>
> *Should we consider an alternative approach? Upgrade one division—one of the smaller ones—and save most of the money while getting a better handle on the benefits of WPA. Or maybe alternative #2 would be to do some of our larger stores—because I think the WPA capability call is a store-by-store decision—to provide better protection where we need it most. Opinions?* [Schuman 2007a]

Even though Butka had a clear understanding of the potential security risks of the older technology, he believed that TJX would save money if they waited further to upgrade its systems. After that initial e-mail, IT staff Lou Julian replied to Butka and colleagues:

> *Saving money and being PCI compliant is important to us, but equally important is protecting ourselves against intruders. Even though we have some breathing room with PCI, we are still vulnerable with WEP as our security key. It must be a risk we are willing to take for the sake of saving money and hoping we do not get compromised.* [Chickowski 2008, p.29]

As weeks went by, another senior-level IT employee had weighed in on this debate. Richard Ferraioli followed up on the e-mail conversation by expressing his concerns on continuing with WEP:

> *The absence of rotating keys in WEP means that we truly are not in compliance with the requirements of PCI. This becomes an issue if this fact becomes known and potentially exacerbates any findings should a breach be revealed.* [Chickowski 2008, p.29]

In the face of the technically-driven debates between IT staff members and Butka, TJX and its management ultimately deferred the investment opportunity and focused on its savings rather than spending.

V. QUITTING E-COMMERCE

Despite the attention and praise from the initial launch of its e-commerce stores, declining sales dampened the promise of innovating their online stores further. In late 2005, the company announced it ceased operations of its online storefronts TJMaxx.com and HomeGoods.com; as a way to return to traditional means of doing business. The closure of these online stores, however, did not mean a collapse of their web presence; they still continued to use those Web sites to operate as “marketing-only Web sites at their same, respective Web addresses” [Business Wire 2005].

Bernard Cammarata had made this key decision as he felt that the e-commerce business did not deliver the expected sales returns as it previously forecast. At this same time, the company had projected pre-tax operating losses at approximately $15 million for the current fiscal year. The main rationale, Cammarata noted was that “exiting this business will eliminate these losses going forward and allow us to better focus our energies into other areas” [Business Wire 2005]. Together with new strategies and real estate expansion to be set for its other stores, the company had other new objectives in mind.

VI. DATA BREACH: THE PERIOD BETWEEN 2005-2006

> *Even with encryption, you still need other measures to make sure you are locking out people who might be the bad guys outside.*
>
> - Chuck Conley, VP, Newbury Networks

Following the closing of its e-commerce storefront, TJX was approached by sales personnel from various security firms. Newbury Networks[1], a company specializing in wireless network security technology, approached TJX to discuss IT security related issues. Knowing that IT security was a growing issue for retailers, they tried to sell their security services to TJX. TJX later declined their offers, responding with a conservative approach to the matter.

Hackers Breach the System

Despite their dismissal, much more was happening in the background. In 2005, on multiple occasions, hackers sat outside of a Marshalls store in St. Paul, Minnesota. Here, they were able to point a telescope-shaped antenna towards the store capturing wireless transactions inside the store as it was being broadcasted through the company's wireless network [Brenner 2007]. In this way, the intruders listened to the traffic through the networks making sure they were invisible and that no one knew they were there. Figure 6 shows a schematic representation of this occurrence.

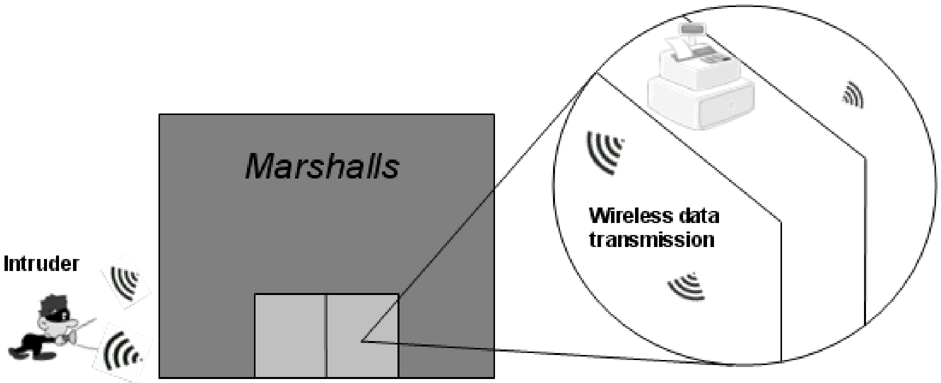


Figure 6. Schematic Representation of Security Breach by the Hackers

[1] Newbury Networks is a wireless network security company who “enables enterprises to locate, manage and secure applications running over wireless LANs (WLANs). Newbury's customers include leading global Fortune 1000 enterprises and public sector government organizations.” http://www.newburynetworks.com/company-about.htm

After listening to this information for two days, the hackers cracked the store's WEP security code. Doing this allowed them to steal credit card information and bank account information. Using this information, between May and December 2006, the hackers regained access into the system and compromised the TJX headquarters' corporate networks in Framingham, Massachusetts. Not only did these hackers infiltrate the system, but they also had access to vital company and customer information from the company's centralized corporate database. The hackers would eventually get away with approximately 45.7 million separate payment cards from transactions dating back to the beginning of January 2003 [Newbury Networks 2008].

Discovery of the Security Intrusion

In early October 2006, TJX retail stores complained about problems with the processing of Discover Card credit cards. Taking action, the company contacted Cybertrust[2] to investigate this matter. After two weeks, the company found that TJX was subject to a breach of data. From the seriousness of the issue and following the suggestion of company attorneys, the company hired General Dynamics and IBM to investigate this matter further [Schuman 2007b].

On December 17, 2006, the hired companies started to investigate the incident. The next day, TJX learned that suspicious software had been detected in its computer systems. By the next week, those investigators determined that the computer systems had been breached and that an intruder remained on the corporate systems. At this time, it was unclear as to who was responsible for the intrusion or whether there was one or multiple, separate intrusions.

Internally, TJX did not find evidence that any of its employees were involved in this incident. The company later confirmed its suspicions that the intruder initially gained access to the system via the wireless local area networks (WLANs) at two stores in St. Paul, Minnesota [Privacy Commissioner 2007].

After analyzing the evidence, TJX notified various U.S. law enforcement agencies of the suspected intrusion. With the agreement of law enforcement, the company informed its contracting banks, credit card, debit card, and check-processing companies of the suspected intrusion. TJX determined that customer information had also been accessed from one of its systems during the computer intrusion [Privacy Commissioner 2007].

Compromised Information

The breached data involved portions of TJX's computer network that contained information from merchandise return transactions from customers of its T.J. Maxx, Marshalls, HomeGoods, and A.J. Wright stores in the U.S. and Puerto Rico. Extending the compromised data further, its Winners and HomeSense stores in Canada were also affected. However, it was not clear if information from its stores in the United Kingdom or Ireland were stolen. Of the stolen information, customers' personal identification numbers (PINs) were not compromised. Even so, it is believed that "drivers' license, military and state identification numbers, together with related names and addresses" provided from returned merchandise without receipts at U.S. and Canadian chains; may have been stolen [TJX Companies 2007]. The company later specifically identified about 455,000 individuals who were in this situation.

In addition, about three-quarters of the 45.7 million cards had either expired at the time of the breach or that the compromised information did not include security-code data from the credit cards' magnetic strips. Because of the extent of the technology used in the intrusion as well as deletions of transaction data from routine system maintenance, TJX believed that it "may never be able to identify much of the information believed to be stolen" [Abelson 2007b; TJX Companies 2007]. The company continued its investigation seeking to determine whether additional customer personal information may have been compromised and, if so, to what extent.

Learning about this incident, chairman Bernard Cammarata along with other executives, ordered the IT department to immediately upgrade their current wireless security infrastructure; both in-store and of its corporate networks. Yet, at the request of law enforcement agencies, the company remained quiet for close to a month before announcing this occurrence to the public.

VII. PUBLIC DISCLOSURE AND FURTHER INVESTIGATION

> *There's a lot we may never know and it's one of the difficulties of this investigation…It's why this has taken this long and why it's been so tedious. It's painstaking.*
>
> - Sherry Lang, PR, TJX Companies Inc.

[2] Cybertrust is a security-services firm based in Virginia. They provide services to businesses such as managed security services, identity management, partner security, and risk assessment. http://www.cybertrust.com/

After immediately alerting law enforcement authorities and maintaining its confidentiality for a while, on January 17, 2007, TJX announced for the first time its data breach to the public. Sherry Lang, the public relations executive, addressed the public and press about the situation. She first mentioned that the company had suffered an unauthorized intrusion of their customer information. Lang also revealed that “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” [Business Wire 2007a].

Both the company and the public were confused at the time as they did not know to the full extent whether the company was breached once or a multiple of times. At the same time, TJX revealed that they were working effortlessly with law enforcement authorities and cooperating with credit and debit card issuers.

A week went by and the card processing companies and press demanded more answers to this serious news. Ben Cammarata later addressed the public in a pre-recorded video message. Full transcript of the message is shown in Appendix IV.

> *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. Our first concern is the potential impact of this crime on our customers, and we strongly recommend that they carefully review their credit card and debit card statements and other account information for unauthorized use. We want to assure our customers that this issue has the highest priority at TJX.* [Boston Globe 2007]

Taking Defensive Action

Under pressure from both credit card companies and the public, TJX vice chairman Donald Campbell commenting on the computer security breach, suggested that it was “similar to that of other large retailers” [Null 2007]. Although the conversations within the IT department were evidence that the company knew about the potential of a security breach, Campbell affirmed:

> *These TJX internal e-mails are just a very small portion of the extensive, ongoing dialogue on the topic of WPA wireless network security and timing of spending which occurred at TJX…TJX decided to move to WPA in advance of being required to do so by the payment card industry. Spending on WPA conversion was not deferred by TJX; in fact, it was accelerated and TJX completed conversion to WPA in advance of its conversion timetable and ahead of many major retailers.* [Null 2007]

Reassuring the Public

Shortly after these announcements, Carol Meyrowitz was named to the CEO position; replacing acting CEO Bernard Cammarata. Despite the negative press coverage and ongoing investigation, she was optimistic about the future of the company stating, “with our goal continuing to be driving profitable sales, TJX has a bright future filled with enormous opportunities” [Business Wire 2007b].

On February 21, 2007, Meyrowitz made a statement to the public concerning information on the computer systems intrusion. She stated:

> *We are dedicating substantial resources to investigating and evaluating the intrusion which, given the nature of the breach, the size and international scope of our operations, and the complexity of the way credit card transactions are processed, is, by necessity, taking time…Additionally, we have strengthened the security of our computer systems. Based on everything we have done, I believe customers should feel safe shopping in our stores…* [Business Wire 2007c]

The company also mentioned that they found evidence indicating that “the intrusion may have been initiated earlier than previously reported; and that additional customer information had possibly been accessed” [Privacy Commissioner 2007]. The company believed “hackers invaded its systems in July 2005, on later dates in 2005, and also from May 2006 to January 2007” [Business Wire 2007c].

Further External Investigation

Since the security breach affected customer data and information of Canadians, the privacy commissioner of Canada intervened and started its own investigation. It was found that TJX breached the collection, retention, as well as security standards in the federal commercial privacy statutes. Concerning TJX’s policies for returning goods and products, the commissioner revealed that the company breached this statue. It also concluded that using this information for fraud control was important, but thought storing this sensitive information was not a necessary step that TJX should have taken [Privacy Commissioner 2007]. The commissioners said:

> *A driver's license is proof that an individual is licensed to operate a motor vehicle; it is not an identifier for conducting analysis of shopping-return habits…Moreover, a driver's license number is an extremely valuable piece of data to fraudsters and identity thieves intent on creating false identification with valid information. For this reason, retailers and other organizations should ensure that they are not collecting identity information unless it is necessary for the transaction.* [Privacy Commissioner 2007]

The investigation further found that TJX did not meet the security standards set by the Payment Card Industry Security Council. The main reason was it had disregarded the upgrade of its wireless security encryption standard within the suggested time frame by the credit card companies. A new version of the PCI DSS was released in September of 2006 and suggested the WPA encryption protocol over the faulty WEP [Privacy Commissioner 2007]. However, TJX should have followed through with the new regulations, but did not. The commissioners commented:

> *TJX relied on a weak encryption protocol and failed to convert to a stronger encryption standard within a reasonable period of time…while TJX took the steps to implement a higher level of encryption, there is no indication that it segregated its data so that cardholder data could be held on a secure server while it undertook its conversion to WPA…If adequate monitoring of security threats was in place, then TJX should have been aware of an intrusion prior to December 2006.* [Privacy Commissioner 2007]

VIII. THE AFTERMATH

In the months following, the company estimated the cost from the computer data breach had soared to $256 million. The accumulation of repairing the company's computer infrastructure, dealing with pending lawsuits, and other claims from the breach added to this cost. However, outside security specialists questioned whether TJX's expenses will be limited to anywhere near the suggested figure [Kerber 2007]. The final bill could increase substantially depending on further investigations and lawsuits which could result in other penalties.

As the investigation continued, and before outside speculation became rampant, TJX disclosed its second-quarter earnings report. Compared to previous years, second-quarter earnings for 2007 lowered the company's profits by $118 million; as a direct result from costs related to the data breach (Figure 7, Appendix V). Months after TJX's announcement, its 2007 quarterly report showed a huge decrease in sales as well as operating income [Leitch 2007].

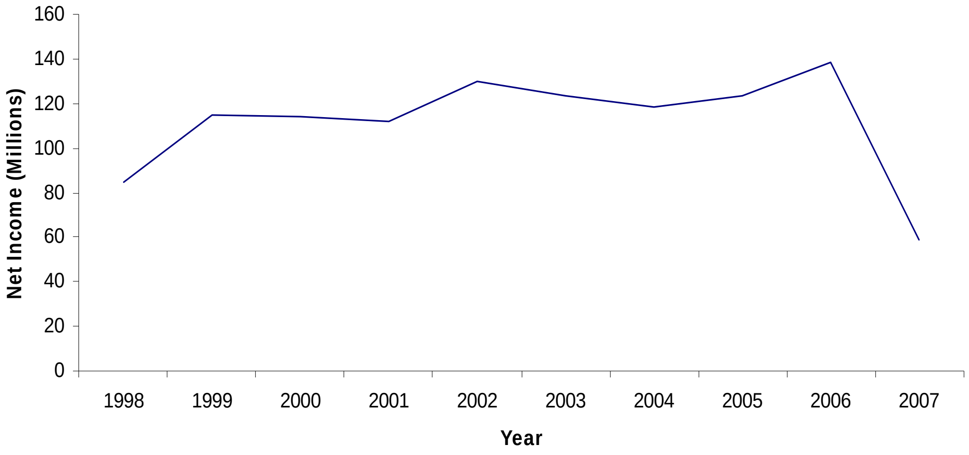


Figure 7. Financial Performance of TJX (Fiscal Second-Quarter Earnings) [Mergent Online 2008]

The Next Steps...

In the months following TJX's February press release, little was heard from the company's senior management. Though, from public information, shareholders have become worried about this news. Second quarter earnings had dropped nearly 57 percent from previous year.

With pending lawsuits from both credit card companies and affected customers; and the loss of shareholder confidence; TJX was faced with a dilemma. The company's next steps to improve its corporate image and to further engage with this problem are still a work in progress.

DISCUSSION QUESTIONS

1. Was it worth the risk TJX took in not upgrading their wireless security standards? Who should be responsible here? Butka? What challenges shall a CIO have for retailers' data security?
2. How should the top management deal with such a situation? Was the press release and video by the chairman sufficient? Did the company disclose enough information to the public?
3. Should IT executives and the IT department be more involved in management decisions? Comment on Butka's role in this situation. Does he have enough power to make a statement?
4. Did TJX retain the information in compliance with PCI DSS and government regulations? Was it the credit card companies' fault for not enforcing stricter guidelines?
5. What social, ethical, and privacy concerns does this case raise? For TJX? For customers?
6. Identify the potential lessons that can be learned from TJX's data breach and any advice you can provide a company in dealing with crisis situations like this one.

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 paper 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.

Abelson, J. (2007a). "TJX Faces Class Action Lawsuit in Data Breach," *The Boston Globe*, January 30, http://www.boston.com/business/globe/articles/2007/01/30/tjx_faces_class_action_lawsuit_in_data_breach/, (accessed March 22, 2008).

Abelson, J. (2007b). "Breach of Data at TJX Is Called the Biggest Ever," *The Boston Globe*, March 29, http://boston.com/business/globe/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/, (accessed March 22, 2008).

Boston Globe Business Team. (2007). "In Video Message, TJX Says It Delayed Reporting for Security Reasons," *The Boston Globe*, March 29, http://www.boston.com/business/ticker/2007/01/in_video_messag.html, (accessed March 25, 2008).

Brenner, B. (2007). "TJX Breach Tied to Wi-Fi Exploits," *TechTarget Security Media*, May 7, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1254020,00.html, (accessed April 1, 2008).

Brodkin, J. (2007). "TJX Breach May Spur Greater Adoption of Credit Card Security Standards," *Network World*, March 29, http://www.networkworld.com/news/2007/032907-tjx-breach-adopt-standards.html?page=2, (accessed March 22, 2008).

Business Wire. (1999). "Nation's Largest Off-Price Fashion Retailer Launches Innovative Web Site," Press Release, November 30, http://www.businesswire.com/portal/site/tjx/, (accessed March 10, 2008).

Business Wire. (2004). "The TJX Companies, Inc. Enters E-Commerce with T.J. Maxx and HomeGoods Web Sites," Press Release, September 23, http://www.businesswire.com/portal/site/tjx/, (accessed March 10, 2008).

Business Wire. (2005). "The TJX Companies, Inc., Reports September 2005 Sales; Announces Exit from E-Commerce Business; Updates Earnings Outlook for Second Half of 2005," Press Release, October 6, http://www.businesswire.com/portal/site/tjx/, (accessed March 11, 2008).

Business Wire. (2007a). "The TJX Companies, Inc. Victimized by Computer Systems Intrusion; Provides Information to Help Protect Customers," Press Release, January 17, http://www.businesswire.com/portal/site/tjx/, (accessed March 12, 2008).

Business Wire. (2007b). “The TJX Companies, Inc. Announces Election of Carol Meyrowitz to Chief Executive Officer,” Press Release, January 30, http://www.businesswire.com/portal/site/tjx/, (accessed March 10, 2008).

Business Wire. (2007c). “The TJX Companies, Inc. Updates Information on Computer Systems Intrusion,” Press Release, February 21, http://www.businesswire.com/portal/site/tjx/, (accessed March 12, 2008).

Chickowski, E. (2008). “Preventing Another TJX,” *Baseline*, (81), February, pp. 22-37

Datamonitor. (2007). “Apparel Retail Industry Profile: United States,” *Datamonitor*, 0072-2005, August, pp. 1-26

Fortune Magazine. (2007a). “Fortune 50 Most Powerful Women in Business 2007,” October 1, http://money.cnn.com/magazines/fortune/mostpowerfulwomen/2007/, (accessed September 22, 2008).

Fortune Magazine. (2007b). “Fortune 500 2007: Full List,” April 30, http://money.cnn.com/magazines/fortune/fortune500/2007/full_list/index.html, (accessed September 29, 2008).

Funding Universe. (2004). “The TJX Companies, Inc.,” Company History, http://www.fundinguniverse.com/company-histories/The-TJX-Companies-Inc-Company-History.html, (accessed March 8, 2008).

Gerling, C. (2006). "WEP vs WPA," *Chris Gerling: Musings of a Security Guru*, June 8, http://www.chrisgerling.com/2006/06/08/wep-vs-wpa/, (accessed March 18, 2008).

Hazari, S. I. (2000). “The Evolution of E-Commerce in Internet Time,” http://www.sunilhazari.com/education/documents/ecomeval.htm, (accessed March 16, 2008).

Hoover's Company Records. (2008a). “The TJX Companies, Inc.,” *In-Depth Records*, March 4, http://www.hoovers.com, (accessed March 4, 2008).

Hoover's Company Records. (2008b). “Kohl’s Corporation,” *In-Depth Records*, September 29, http://www.hoovers.com, (accessed September 29, 2008).

Hoover's Company Records. (2008c). “Macy’s, Inc.,” *In-Depth Records*, September 29, http://www.hoovers.com, (accessed September 29, 2008).

Internet Archive. (2008). “T.J. Maxx,” Web Site Archives, http://www.archive.org/, (accessed March 25, 2008).

Kerber, R. (2007). “Cost of Data Breach at TJX Soars to $256m,” *The Boston Globe*, August 15, http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/, (accessed March 15, 2008).

Leitch, S. (2007). “TJX Profit Down 57% on Credit-Card Theft Loss Reserve,” *MarketWatch*, August 14, http://www.marketwatch.com/news/story/tjx-profit-down-57-credit-card/, (accessed March 26, 2008).

Mergent Online. (2008). “TJX Companies, Inc.,” *Company Financials*, http://www.mergentonline.com, (accessed March 25, 2008).

Newbury Networks. (2008). “Company Overview,” http://www.newburynetworks.com/, (accessed March 10, 2008).

Null. (2007). “TJX E-Mails Tell the Tale,” *Daily Online News*, November 29, http://dailyscooponline.blogspot.com/2007/11/tjx-e-mails-tell-tale.html, (accessed March 15, 2008).

O'Rourke, M. (2005). “Data Security in Crisis,” *Risk Management*, (52:5), May, pp. 9-9

PCI Security Standards Council. (2006). “Payment Card Industry (PCI) Data Security Standard,” https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf, (accessed March 15, 2008).

Privacy Commissioner of Canada. (2007). “Report of an Investigation into the Security, Collection and Retention of Personal Information,” Office of the Privacy Commissioner of Canada, Report of Findings, September 25, http://www.privcom.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp, (accessed March 25, 2008).

Schuman, E. (2007a). “VISA Fined TJX Processor $880,000 For Security Violations,” *Storefront Backtalk*, October 27, http://storefrontbacktalk.com/story/102707visafine, (accessed April 1, 2008).

Schuman, E. (2007b). “Attorney: TJX Knew of Data Breach Earlier Than It Claims,” *eWEEK*, December 14, http://www.eweek.com/c/a/Security/Attorney-TJX-Knew-of-Data-Breach-Earlier-Than-It-Claims/, (accessed March 18, 2008).

The Associated Press. (2008). “Credit Card Breach Raises Broad Concerns,” *The New York Times*, March 23, http://www.nytimes.com/2008/03/23/us/23credit.html?_r=1&oref=slogin, (accessed April 1, 2008).

The TJX Companies, Inc. (2007). “The TJX Companies Inc. 2006 Annual Report,” http://www.tjx.com/ir/ar.html, (accessed March 25, 2008).

TJX Companies, Inc. (2007). “Frequently Asked Questions,” September, http://www.tjx.com/tjx_faq.html, (accessed March 22, 2008).

Turban, E., J. K. Lee, and H. M. Chung. (2000). *Electronic Commerce: A Managerial Perspective*, Upper Saddle River, NJ: Prentice Hall.

Velte, T. J. and A. T. Velte. (2006). *Cisco 802.11 Wireless Networking Quick Reference*, Indianapolis, IN: Cisco Press.

APPENDIX I: HISTORY OF TJX COMPANIES, INC.[3]

Year	Event
1956	First Zayre discount store was founded by Stanley and Simmer Feldberg
1962	Chain stores were Incorporated as Zayre Corp.
1977	First TJ Maxx was opened
1987	TJX Companies, Inc. was established as subsidiary of Zayre Corp.
1988	Zayre Corp. was divested and renamed as TJX Companies, Inc.
1990	TJX acquired Winners Apparel Ltd., a Canadian chain
1992	Launch of the HomeGoods fashion chain
1994	Ventured into United Kingdom, launched T.K.Maxx
2001	Operated HomeSense, a Canadian version off HomeGoods
2004	Headquartered in Framingham, Massachusetts

APPENDIX II: GENERAL COMPANY INFORMATION[4]

A. Company Information

Legal Status:	Public
Ticker Symbol:	TJX
Employees:	125,000
Fortune 500 Ranking:	133

B. Global Markets

Country	No.
United States	2,004
Canada	252
United Kingdom	202
Ireland	8

C. Number of Stores

Store Brand	No.
T.J. Maxx	821
Marshalls	748
HomeGoods	270
T.K. Maxx	210
Winners	184
A.J. Wright	129
HomeSense	68
Bob's Stores	36
Total	2,466

APPENDIX III: PCI’S 12 REQUIREMENTS FOR RETAILERS[5]

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

[3] Adapted from: Hoover's Company Records. (2008) “The TJX Companies, Inc.”, In-depth Records, http://www.hoovers.com, (accessed March 4, 2008).

[4] Ibid.

[5] Adapted from: PCI Security Standards Council. (2006) “Payment Card Industry (PCI) Data Security Standard”, https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf, (accessed March 15, 2008).

7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

APPENDIX IV: BEN CAMMARATA'S VIDEO MESSAGE TO ITS CUSTOMERS[6]

"I'm Ben Cammarata, Chairman and founder of the TJX Companies. I've devoted much of my adult life to building this company. And the recent unauthorized intrusion into our computer systems disturbs me greatly, as I'm sure, it does to you.

We opened our first two stores 30 years ago. And since day one, our company has stood for great value. And above all else, we value you our customers. I cannot tell you how deeply I regret any difficulties that our customers may be having because of this problem.

The first thing I'd like to do is to give you a quick overview of the many steps we've taken since learning about the systems intrusion. We immediately engaged two leading computer security firms to investigate the problem and enhanced our computer security in order to protect our customers' data. We also notified law enforcement authorities who began the investigation of the crime. We have worked very closely with the major credit card companies on this matter. We've provided them with the information they've requested to protect the customers whose credit and debit card information may have been compromised. Further, we've established customer help lines in three countries and made available a great deal of helpful information on all of our company Web sites. We've been listening to our customers' questions as you've been calling our help lines. And we've updated our Web sites as new information becomes available.

I want to take this time to address some of the key issues that seem to be on people's minds. You've asked us why did we not announce the systems breach until mid-January when we discovered them in December. Well, first and foremost, we were concerned that there would be an expansion of the systems breach. By not making the public announcement in December, and with the help of top security experts, we were able to contain the problem and strengthen our computer network to prevent the possibility of further intrusion and of future attacks by the intruder or others like him. Most importantly, our actions greatly reduced the risk for more customer data to be exposed. Therefore, we believe that we were acting in the best interest of our customers. In addition, we maintained confidentiality of the intrusion as requested by law enforcement.

Another question some of you have asked is why the company isn't contacting our customers directly about this problem. The simple answer is most of the information that was or may have been stolen did not include customer names and addresses. When customers conduct debit and credit card transactions in our stores, we don't collect their names and addresses. Most of the data that may have been compromised in the breach was credit and debit card numbers and expiration dates. Also, we are fairly certain that debit card personal identification numbers or PINs were not compromised. We've provided these credit and debit card numbers to the banks and to the credit card companies. We have a relatively small number of customers whose names, addresses, and driver's license numbers we know were stolen in the intrusion. This information was provided in the returns of merchandise without receipts. I have personally sent letters to them. And we have set up a dedicated help line for them.

One point that I'd like to make is that criminals use situations like this to scam you the public. Consumers need to be wary of scams, hoax e-mails, and calls in which they are contacted by someone claiming to represent TJX. I assure you we would never solicit personal information via phone or e-mail.

This leads me to talk about another customer concern that has come up. And that is identity theft. The leading experts in this area tell us that it would be extremely unlikely for cyber-thieves to commit identity fraud with the information that was breached in this incident. Most of the information at risk does not include names or addresses.

[6] Image and Transcript adapted from: Boston Globe Business Team. (2007) "In video message, TJX says it delayed reporting for security reasons", The Boston Globe, http://www.boston.com/business/ticker/2007/01/in_video_messag.html, (accessed March 25, 2008).

We never request customers' social security numbers in our transactions which is usually a critical piece of information needed to commit identity theft.

Some customers have asked us why we had not offered to pay for credit monitoring. Based on the type of data involved in the breach of our systems, we don't believe that such monitoring would be meaningful to customers. In other words, credit monitoring does not detect fraudulent charges on your credit and debit card accounts. Although banks and credit card companies generally monitor for fraud, your best defenses is careful review of your own statements. And that is why I urge you to strongly do so.

There have been two developments since our January 17th announcement that we are now able to share with you. First, based on our investigation, we now believe that customer transactions at Bob's Stores were not involved in the systems intrusion. Also, we can now report that we do not believe that transactions using debit cards issued by Canadian banks were involved in the systems breach.

Over the years, I've been in hundreds of our stores, and I know I've met a lot of you. We have never taken your business for granted, and we never will. Those of you who know us know that we care. We will not allow this unfortunate incident to blur what we are all about. And that is: the trust we've built with our loyal customers, our community involvement, and the dedication of our 120,000 TJX associates worldwide.

Customers should realize today there really is no computer system that is completely safe from sophisticated criminals. Broadly speaking, computer systems security is a very complex issue. It involves not just retailers, but banks, credit card companies, trade associations, government agencies, and so on.

We have taken extraordinary measures with the nation's leading computer security experts to further strengthen the safeguards within our systems. We want our customers to feel safe shopping at our stores. And I really believe you are.

I want you to know that all of our associates have remained focused and are working hard to provide you with the great values and the service you've come to expect from us. Once again, I regret any difficulties our customers may have experienced because of this incident. I hope I've been helpful in answering some of your questions and we will continue to update you as we gather more information.

Thanks for bearing with us through this very challenging situation. And thank you for your loyalty over the years."

APPENDIX V: COMPARISON OF COMPANY EARNINGS FOR 2006 AND 2007[7]

Figures from Quarterly Income Statements (in millions)	2nd Quarter (2007)	1st Quarter (2007)	3rd Quarter (2006)	2nd Quarter (2006)	1st Quarter (2006)	3rd Quarter (2005)
Net sales	4,313.30	4,108.08	4,501.07	3,988.23	3,896.48	4,041.91
Cost of sales	3,277.70	3,117.22	3,356.76	3,054.47	2,942.78	3,065.06
Selling, general & administrative expenses	749.05	709.28	762.14	698.78	689.54	687.38
Provision for Computer Intrusion related cost	195.92	20.004	-	-	-	-
Net income	59.03	162.11	230.61	138.16	163.81	171.16

[7] Mergent Online. (2008) "TJX Companies, Inc.", Company Financials, http://www.mergentonline.com, (accessed March 25, 2008).

ABOUT THE AUTHORS

William Xu is currently completing his Professional MBA in Financial and Technology Management from the Sprott School of Business at Carleton University. His research interests include Management in Information Systems and Technology. He has a B.Sc. in Biotechnology from the University of Ottawa. During his studies, he is the co-founder of the University of Ottawa Computer Club where he holds information seminars on emerging technology topics.

Gerald Grant is an Associate Professor and Coordinator of the Information Systems Area at the Sprott School of Business, Carleton University. He holds a Ph.D. in Information Systems from the London School of Economics and Political Science, University of London, UK. His research interests include enterprise-wide and global information systems, electronic commerce and international electronic collaborative networks, and information systems in developing countries. In addition to teaching and research, he has consulted for the Commonwealth Secretariat in the UK and the COMNET-IT Foundation in Malta on projects related to e-business and e-government IT strategies and institutional networking. He is editor of two books, *Managing Telecommunications and Networking Technologies in the 21st Century: Issues and Trends*, and *ERP and Datawarehousing in Organizations: Issues and Challenges*; both published by Idea Group Publishing.

Hai Nguyen is currently pursuing his MBA at Carleton University's Sprott School of Business with a concentration in Financial Management. He holds a B.A. in Economics. His research interests are in Financial Management, International Business, and Technological Innovation.

Xianyi Dai is a Financial Advisor at TD Canada Trust. She has a B.A. in General Social Sciences and is currently completing her Professional MBA at the Sprott School of Business at Carleton University with a concentration in Technology Management and Finance.

Communications of the Association for Information Systems

ISSN: 1529-3181