Project 1: The TJX Data Breach
Katie Zurowski
CFRS 664: Incident Response

Part 1: The Incident

The details of the TJX intrusion sound more like a high-tech sequel to Ocean's Eleven than real events. It begins with a government informant returning to a life of crime, includes a flash drive described as a "safety precaution" in case of blackmail, and ends in the aftermath of a dramatic arrest at a Turkish nightclub[1]. The impact of the intrusion was almost as dramatic as the events themselves. TJX admitted that over 45 million credit card number had been stolen from their companies, the largest loss of personal credit card data in history at that time[2]. It's now widely accepted though that the actual number of lost cards is twice that estimate. The losses cost TJX over $250 million[3], and damaged the company's public image. The saving grace for TJX companies was that soon the intrusion was eclipsed by other, even bigger losses of personal data.

Albert Gonzalez, the man who coordinated the TJX intrusion, was picked up in 2003 at an ATM in New York City for using stolen credit cards to withdraw cash. He stood at the machine and inserted card after card, withdrawing the daily maximum on each. He was able to avoid prosecution for "cashing", as it's called, when officials realized that he had both the skills and the connections to help them infiltrate the online stolen credit card market. However, within two years, he had finished a major operation with the U.S. Secret Service and had begun experimenting with new vulnerabilities to gain illegal access to corporate networks[1]. Figure 1, below, outlines the major events between July 2005 and December 2006, when Gonzalez and his associates infiltrated the TJX network.

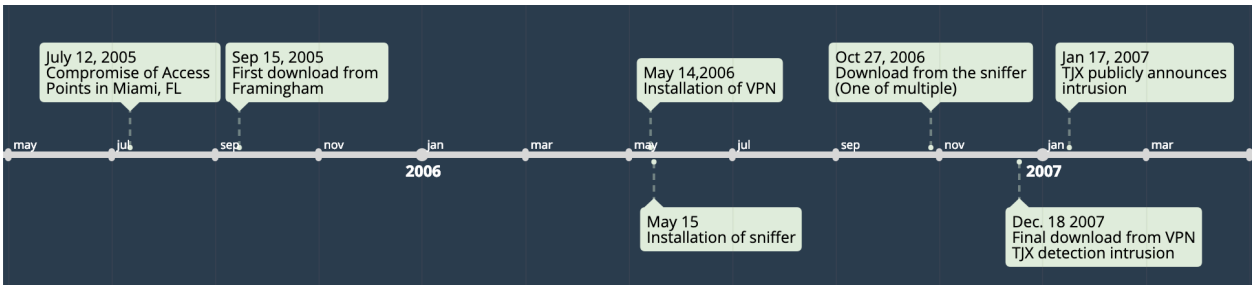

Figure 1. Timeline of events

The first event that directly impacted TJX occurred on July 12, 2005. Albert Gonzalez and Christopher Scott "compromised two wireless access points operated by TJX at Marshalls department stores in Miami, Florida", according to his indictment[4]. The two had been experimenting with a reconnaissance technique known as "war driving"[1]. War driving uses scanners to search for frames sent out by access points when a device attempts to connect to it. These frames are broadcast out over the network and are easy to pick up with the right equipment. The attackers are able to see information about the network, including its security settings[5].

In 2005, TJX stores were using the Wired Equivalent Privacy (WEP) Standard for their in-store wireless networks. This network connected various devices within the store, including their price scanners and Point of Sale Devices. The encryption mechanisms used in WEP were already considered unsecure, and the two were able to access the internal store network with relative ease. Once inside, they were able to see internal traffic (including employee usernames and passwords) and move laterally into the central servers in Framingham, MA[6].

While in this network, the attackers "downloaded payment card data stored on TJX's servers in Framingham" on multiple occasions, including Sep 15 and Nov 18[4]. However, this data proved disappointing. The company's policy of deleting data meant that much of the data in Framingham has persisted there for several years. Many of the card numbers exfiltrated had expired and could not be sold online[1]. However, the network was vulnerable enough that it showed promise for other types of data collection.

By the following May, the attackers had formulated a new strategy to maximize their efforts. They "installed a VPN connection from a TJX payment card transaction processing server" to a personal server. Next, they deployed custom sniffer programs onto the compromised server[4]. This program recorded transactions that were processed on the server and collected them until the file reached a certain size. Once it passed the threshold, it encrypted and compressed the file, and send it over the VPN to the attackers' server[1].

This method exploited a major vulnerability in TJX's card processing. During the payment card approval process, the customer's credit card data was sent from the store to card issuer unencrypted[6]. This meant that anyone with access to the TJX network could collect the customer credit card information by simply listening in; and that is exactly what Gonzalez and his associates did.

This sniffer program was able to run with little to no human interaction, meaning the attackers could shift their focus to other things. This included packaging and selling the card numbers online from TJX and other intrusions the group had in progress[4]. Automated downloads occurred several times throughout the rest of 2006.

TJX spent the entirety of this time completely unaware that any kind of attack had even occurred. In December 2006, TJX was contacted by a credit card company, informing them that an increasing number of credit cards used in store were apparently stolen[1]. The team immediately began a security audit and, on December 18 an auditor discovered an anomaly in the company's credit card data.

December 18 was also the date of the final data download over the VPN to the attackers' server. However, it is unclear whether the company shut down the link when they discovered it that day, or if the attackers realized they had been detected and withdrew on their own. It is believed that the attackers knew they had been detected, and did not attempt any new downloads after that date[6].

The company contracted two external response team from International Business Machines Corp. and General Dynamics Corp. to carry out their incident response activities. On December 22, the company alerted law enforcement, and the U.S. Secret Service began an investigation into the intrusion. The company stated in an SEC filing that:

> "U.S. Secret Service advised us that disclosure of the suspected Computer Intrusion might impede their criminal investigation and requested that we maintain the confidentiality of the suspected Computer Intrusion until law enforcement determined that disclosure would no longer compromise the investigation"[7].

One month after discovering the incident, TJX announced publicly that its systems had been attacked. Their original statements claimed that the incident affected, "a limited number of credit and debit card holders"[6]. They released an "Important Customer Alert" on their webpage from the acting CEO, which stated the company was "extremely disappointed" when it discovered the intrusion[8]. The company resisted providing an estimate of how many customers were affected by the incident until well into March of 2007. They finally announced that 45.6 million credit and debit card numbers had been exfiltrated during the intrusion[2].

Tracking down Gonzalez and his associates proved to be a year-long game of cat-and-mouse. An associate was arrested in North Carolina and found with a flash drive that contained Gonzalez's personal information. The associate planned to use it if Gonzalez began to work with the police again. This associate had been previously arrested in early 2005 while sitting in a shopping center parking lot in the middle of the night with Christopher Scott and a large radio antenna[1]. The two were almost certainly refining the "war driving" technique that would later be used in the attack. However, at the time there was no connection between this associate and TJX.

Gonzalez was funneling most of his stolen card numbers through another associate in Ukraine. He continued to do so even after he knew that this associate was being investigated by the police because of the US's lack of extradition policies with Ukraine. However, he didn't plan for the associate to take a vacation to Turkey, where he was arrested for selling credit card numbers to an undercover Secret Service agent. His records led police to an Instant Messaging account who

had been providing him with the bulk of his card numbers, including those from TJX. When the Secret Service managed to find registration information for the messaging account, it linked to one of Gonzalez's many known aliases[1]. He was finally arrested in May 2008 and is serving a 20-year sentence[9].

Part 2: The Response

The sheer size of the data lost in the attack on TJX led to public outcry. It quickly became known as the largest data breach of all time. As information began pouring in about both the breach and TJX's company practices, there was no denying that TJX failed in many aspects of their incident response. Their corporate response after the attack was lackluster and insincere. But worse still, their total failure to protect against attacks made them a prime target.

As soon as TJX announced that they had detected an attack, the public began to wonder why they had waited so long to inform the affected individuals. Originally, TJX stated that they waited a month to comply with the requests of law enforcement, as stated in their 2007 10-K report (quoted in Part 1). However, they later admitted that they delayed notifying the public partly as a "business decision". People did not hesitate to make the connection that the company conveniently waited until after the Christmas shopping season had finished. Whether or not they intentionally chose to wait until after Christmas so the attack would not harm sales, this was a poor start for the company's public relations in regards to the incident.

There is little published on the internal investigation that occurred once TJX discovered the breach. They did hire two external incident response teams, instead of creating an internal team. This decision shows that they at least recognized that they were ill-equipped to handle a breach internally, and made took decisive action to ensure the investigation could be carried out properly.

However, the investigators may not have had much with which to work. They were able to determine that the attackers pulled approximately 100 files from the servers in Framingham. They also even found messages that the attackers had left on the server, communicating which files had been copied already and which hadn't[1]. However, many of these files had been deleted during the 18 months the attackers had access to the system, and it was impossible to tell what was in them. Looking at the dates of the transaction compared to the time of the attack, the company may have been holding data in Framingham for over two years[10].

According to TJX, these files were deleted as part of the standard operating procedure before the attack was discovered[10]. While this may be partly due to the amount of time the attackers were in the system (and these files were downloaded at the beginning of the attack), if TJX had deleted these files more regularly, they would not have been available in the first place. It's unclear what the actual policy was for file retention, or if there was any consistent practice for the files housed in the Framingham servers at all. Their file retention policy is the first of many pieces of evidence that TJX's security posture before the attack was severely lacking.

Additionally, security expert Michael Maloof speculated that "TJX did not have the log data needed to do a proper forensic analysis of the incident"[11]. This has led many analysts to believe that the true number of compromised customers is a high as 94 million. Bank record and TJX's internal records show discrepancies that more than double the company's estimate of the number of compromised customers. TJX maintained their estimate but seemed to undercut that statement by saying that most of the accounts stolen were expired anyway[12], possibly implying that they did not include the expired accounts in their estimate. Again, TJX's statements and investigation failed to satisfy customers and security experts. Additionally, by 2009, the estimate of 94 million had become the widely accepted number of compromised accounts[2].

However, the true failing of the company was their non-compliance with Payment Card Industry (PCI) standards. Adherence to PCI standards was mandatory for any business processing credit cards starting in 2004[13]. This included time limits on data retention, which TJX was clearly not following, as mentioned above. It is difficult to believe that over a two-year period the company did not realize that they were non-compliant. In September of 2006, it is eve on record that an auditor informed the company they were not compliant with the standards[6]. However, there was no indication that the company planned to make changes to become compliant after the report. It is unclear whether any of the credit card companies that required PCI compliance had been notified, or if they planned action against TJX, because by December the breach had been detected.

The company was also still using WEP security for their in-store Wifi networks, as noted in Part 1. The same security flaws that were exploited by the attackers had been identified as early as

2001, and by 2003 Wifi Protected Access (WPA) had been introduced. WPA improved on the vulnerabilities that existed in WEP, including the weak password encryption. While WPA was not mandatory, many merchants had made the switch to improve their network security[6].

The impact that affected TJX the most directly though was the simple monetary cost of the breach. They had to cover the fees for hiring two external response teams, legal fees for several litigations over a period of several years, costs associated with becoming PCI compliant, and general security improvements. The company was also required to cover the fraud losses of both Visa and Mastercard, $40 million and $25 million respsectively[13]. By 2009, the company had paid $256 million in response to the breach[2]. The company did not disclose the cost of increasing their internal security, but it is easy to assume that it was vastly lower than the final payout accumulated throughout their response process. Their failure to prepare for an incident resulted in a direct impact to the business on a scale they clearly did not anticipate.

In sum, TJX's mistakes in their handling of the attack can be placed into two categories. First, they failed to properly identify their risks and critical assets. Even if they did carry out an assessment of critical assets, they did not properly identify their information assets as critical. Some believe this may be because "information practices are ancillary to its core business as a retailer"[13], and they did not see a connection between their data and their business. This led to a cascading effect through their policies and practices that set them up for failure from the start. The company failed to detect the attackers throughout the entire 18 month period and had to be notified of suspicious activity from an outside entity. They also failed to set up an infrastructure that allowed them to do proper forensic work. Their logging appears to have been inconsistent, so they could not track the attackers' activity in the network.

Second, their response to the attack deeply damaged their reputation. Their repeatedly refused to take responsibility for the vulnerabilities that led to the attack, even as they admitted they were non-compliant with industry security requirements and standards. Their public statements seemed to prioritize their business over their customers. For example, looking at the details of their public response, I agree with the belief that they withheld informing the public about the breach until after Christmas so that they could avoid bad press during peak season.

Security columnist Scott Bradner provided a poignant comparison of the incident. He compared the TJX breach to the Tylenol deaths of 1982, stating that the company had the opportunity to rise to the occasion of a damaging incident and "get in front of the issue and stay there"[14]. However, TJX failed to fully take responsibility for the intrusion, and their reputation suffered for it. Within only a few years though, the breach was overshadowed by bigger or more dramatic attacks. It now stands as a piece of modern history as "the first major breach of the information era", and the lackluster response is looked at as simply a case study for poor management.

References:

[1] Verini, J. (2010, November 10). The Great Cyberheist. *The New York Times Magazine.* Retrieved March 11, 2019, from https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html

[2] TJX hacked to the max: 45 million cards. (2007). *Computer Fraud & Security, 2007*(4), 2-3. doi:10.1016/s1361-3723(07)70054-4

[3] Cheng, A. (2013, December 13). Target admits 40 million cards are compromised; TJX's 2007 breach cost $256 million [Web log post]. Retrieved March 11, 2019, from https://blogs.marketwatch.com/behindthestorefront/2013/12/19/targets-card-breach-delivers-a-rude-christmas-surprise/

[4] United States of America vs Alberto Gonzalez (United States District Court: District of Massachusetts August 5, 2008).

[5] Kern, B. D. (2004). Whacking, joyriding and war-driving: Roaming use of wi-fi and the law. *Computer & High Tech Law Journal, 21*, 101-162. Retrieved March 11, 2019.

[6] Pereira, J. (2007, May 4). How Credit-Card Data Went Out Wireless Door. *The Wall Street Jouranl*, p. A1. Retrieved March 11, 2019, from http://online.wsj.com/article_print/SB117824446226991797.html

[7] TJC Companies, Inc. (n.d.). *Form 1-K* [SEC Filing]. Retrieved March 11, 2019, from http://www.tjx.com/investors/filings-and-presentations/annual-reports

[8] Cammarata, B. (2007, January 25). Letter From TJX's Chairman and Acting CEP. Retrieved March 11, 2019, from https://web.archive.org/web/20070125160834/http://www.tjx.com/tjx_message.html

[9] Leader of Hacking Ring Sentenced for Massive Identity Thefts from Payment Processor and U.S. Retail Networks. (2014, September 16). Retrieved March 11, 2019, from https://www.justice.gov/opa/pr/leader-hacking-ring-sentenced-massive-identity-thefts-payment-processor-and-us-retail

[10] Sullivan, B. (2007, March 29). TJX Hack: More of the Same. Retrieved March 11, 2019, from http:/redtape.msnbc.com/2007/03/tjx_hack_more_o.html#posts

[11] Vennamaneni, M., & Vennamaneni, M. (2016, February 21). Security Breach at TJX - Analysis. Retrieved March 11, 2019, from https://medium.com/@mounicav/security-breach-at-tjx-analysis-675a0fb1cedf

[12] Kaplan, D. (2018, July 05). Banks: TJX lost twice as much data as reported. Retrieved March 11, 2019, from https://www.scmagazine.com/home/security-news/banks-tjx-lost-twice-as-much-data-as-reported/

[13] Culnan, & Williams. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches. *MIS Quarterly, 33*(4), 673. doi:10.2307/20650322

[14] Bradner, S. (2007, January 29). TJX security breach aftermath: A case study in what to do wrong. Retrieved March 11, 2019, from https://www.networkworld.com/article/2303490/tjx-security-breach-aftermath--a-case-study-in-what-to-do-wrong.html