


Lessons learned from the TJ Maxx Data Breach

TJ·maxx



We will be discussing the TJX (owners of retailers TJ Maxx and Marshalls) security breach in this case study , and we thought it might be useful to see **what has been learnt from what is now described as the biggest data security breach ever.**

Lessons learned from the TJ Maxx Data Breach

■ About T.J Maxx



T.J. Maxx was founded in 1976, and together with Marshalls, forms **The Marmaxx Group**, the largest off-price retailer of apparel and home fashions in the **U.S.** T.J. Maxx sells brand-name family apparel, including women's footwear and active wear, home fashions and other merchandise such as beauty and **operated from approx. 900 stores.**

Lessons learned from the TJ Maxx Data Breach

■ Executive Summary



In January 2007 TJ Maxx announced that millions of customers might have been affected by a data breach that was undiscovered since 2005. To make matters worse the data breach may have been the result of a simple security oversight - failing to secure a wireless network at a discount store.

Lessons learned from the TJ Maxx Data Breach

■ Background



According to the Wall Street Journal - "The \$17.4-billion retailer's wireless network had less security than many people have on their home networks, and for 18 months the company - had no idea what was going on. The hackers downloaded at least 45.7 million credit- and debit-card numbers from about a year's worth of records, the company says. A person familiar with the firm's internal investigation says **they may have grabbed as many as 200 million card numbers all told from four years' records.**"

Lessons learned from the TJ Maxx Data Breach

■ Cost Impact



TJ Maxx later estimated in its SEC filings that the breach would cost the company around \$5 million. But security experts place the potential long-term cost as high as \$4-\$8 billion. In additions to fines, recovery costs, and brand damage, TJ Maxx was also being sued by more than 300 banks and credit unions.

Lessons learned from the TJ Maxx Data Breach

■ Findings



While most organization that take credit cards use some form of encryption to protect data during and after the transaction, it appears that **not only were the TJX thieves able to intercept customer credit card data before it was encrypted, the bad guys also had a copy of the encryption key anyway.** According to one security analyst it's like locking the door and leaving the key under the mat. And word is out that **TJX was also not compliant with PCI-DSS** introduced to protect cardholder data in retail.

Lessons learned from the TJ Maxx Data Breach

■ Story behind



Albert Gonzalez, the computer hacker behind one of the largest known identity fraud cases in U.S. history, was sentenced to 20 years in federal prison. Gonzalez, a 28-year-old college dropout and Secret Service informant known as "soupnazi," had confessed to **stealing millions of credit card and debit card numbers from major U.S. retail chains, including T.J.Maxx, BJ's Wholesale Club, and Barnes & Noble.**

Lessons learned from the TJ Maxx Data Breach

■ Story behind



In August 2008, Gonzalez , along with 10 others from the United States, Eastern Europe, and China, convicted of breaking into retail credit card payment systems by **wardriving** --that is, using a laptop to detect retailers' unsecured wireless networks--and installing sniffer programs to capture data.

Lessons learned from the TJ Maxx Data Breach

■ Story behind



Gonzalez and his alleged co-conspirators sold the credit numbers, encoded the data onto magnetic stripes of blank cards including gift cards, and used the new cards **to do tens of thousands of dollars fraudulent transactions at a time**. They also allegedly concealed and laundered their proceeds by using anonymous Internet-based currencies within the United States and abroad, and by channeling money through bank accounts in Eastern Europe. Separately, New Jersey prosecutors say Gonzalez conspired to steal credit card numbers **from Heartland Payment Systems, 7-Eleven, and supermarket chain Hannaford Bros.**

Lessons learned from the TJ Maxx Data Breach

■ Litigation and Settlement

Litigation revealed that TJX was not compliant with **nine of the twelve PCI DSS requirements covering encryption, access and firewalls.**

On June 23, **TJX settled the action with 41 state Attorneys General for \$9.75 million.** In addition to monetary payments, the June 23 agreement requires TJX to implement a comprehensive **"Information Security Program, including PCI-DSS"** to protect the security, confidentiality, and integrity of Personal Information.

Lessons learned from the TJ Maxx Data Breach



- As retailers and financial institutions we are responsible to our customers for protection of their data.