

Analyzing the TJ Maxx Data Security Fiasco

Lessons for Auditors

By Gary G. Berg, Michelle S. Freeman, and Kent N. Schneider

AUGUST 2008 - In January 2007, TJX Companies, Inc. (TJX), the parent company of retail chains such as T.J. Maxx and Marshalls, issued a press release announcing that its computer systems had been breached and that customer information had been stolen. As the investigation into the crime continued during 2007, estimates of the number of customers affected skyrocketed. Other reports indicated that at least 94 million Visa and MasterCard accounts had been compromised, with losses projected to approach \$4.6 billion. As expected, Visa and MasterCard are seeking to recoup these losses from TJX. The sheer scale of the security breach should cause auditors to wonder about the implications for their professional practice.

What Went Wrong at TJX?

Investigations into the TJX case appear to indicate that the company was not in compliance with the Payment Card Industry (PCI) data security standards established in 2004 by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. Reports identified three major areas of vulnerability: inadequate wireless network security, improper storage of customer data, and failure to encrypt customer account data.

Inadequate wireless network security. The store where the initial breach occurred was using a wireless network that was inadequately secured. Specifically, the network was using a security protocol known as wired equivalent privacy (WEP). One problem with WEP security is that it is easy to crack. In fact, researchers at Darmstadt Technical University in Germany have demonstrated that a WEP key can be broken in less than a minute. More important, WEP does not satisfy industry standards that require the use of the much stronger WPA (Wi-Fi Protected Access) protocol. After breaking into the store's network, the hackers then breached security at the corporate headquarters and obtained the customer account information stored there. According to a May 4, 2007, *Wall Street Journal* article, the intruders had access to the TJX records for 18 months without being detected.

Improper storage of customer data. The TJX data storage practices also appear to have violated industry standards. Reports indicate that the company was storing the full-track contents scanned from each customer's card. Moreover, customer records appear to have included the card-validation code (CVC) number and the personal identification numbers (PIN) associated with the customer cards. PCI Data Security Standard 3.2 clearly states that after payment authorization is received, a merchant is not to store sensitive data, such as the CVC, PIN, or full-track information. [Exhibit 1](#) shows a comparison of key data items believed to have been stored by TJX, along with the relevant PCI standards.

Most likely, TJX did not retain this information with malicious intent. The company may have been using older point-of-sale (POS) software that had been designed to capture all card data and that could not be reconfigured to comply with PCI standards.

This problem has been linked to credit-card security breaches at other retailers. Another possibility is that the POS software was adequate, but improperly configured.

Failure to encrypt customer data. Even if the hackers had been able to infiltrate the TJX corporate network and access the improperly stored customer records, it is likely that no harm would have resulted, had the customer data been securely encrypted. Given the large number of fraudulent transactions traced back to the TJX breach, it is obvious that either the data had not been encrypted, or the hackers stole the encryption key. In either case, industry standards were not maintained by TJX. PCI Data Security Standard 3.2 requires that at minimum, the customer's "primary account number" (i.e., the customer's card number) be "rendered unreadable." Furthermore, PCI Data Security Standards 3.4 and 3.6 require merchants to protect the encryption keys used for protecting customer data from disclosure and misuse.

How the TJX Breach Affects Audit Practices

At first, the TJX fiasco appears to offer an object lesson for retailers' IT departments, rather than auditors. After all, customers' credit card numbers are not the retailer's asset to protect; rather, the sales transaction itself is what accounting internal controls have traditionally sought to secure. With the advent of Statement on Auditing Standard (SAS) 109, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, internal control clearly extends beyond protecting one's own assets.

SAS 109 requires auditors to "audit the business, and not just the books" when evaluating the risks of a client's financial statements containing a material misstatement. Specifically, SAS 109 requires an understanding of: 1) the entity and its environment; 2) the entity's internal control environment; and 3) susceptibility of the entity's financial statements to material misstatement resulting from liabilities.

Understanding the entity and its environment. Retailers cannot continue to operate by looking after only their own assets, as seen in the TJX debacle. Customer credit and debit card information is a valued target of data thieves. Technology has made purchasing information more valuable than actual currency, because it can be used to run up huge bills for the original cardholders. These victims are left with the lengthy, painful task of restoring their good credit ratings. To protect against data theft, consumers can refrain from using debit and credit cards (an inconvenient option), or refrain from shopping at stores that suffer data breaches. In other words, it is ultimately in the best interest of retailers to follow industry standards and protect customer credit and debit card records.

Understanding the entity's internal control environment. In the digital economy, retailers must implement both physical and electronic controls. For example, stores should have physical control over the credit card scanners at checkout locations by bolting them to the counter. Otherwise, a thief could replace a retailer's scanner with an identical-looking scanner that also stores scanned customer information on a hidden chip. Later, the thief could return to the store and switch scanners again, walking away with the customer data accumulated in the interim.

Understanding the risk of material misstatement resulting from contingent liabilities. Although customer purchasing information is not an asset of the retailer, possession of that information imposes great responsibility on the retailer, and failure to protect that information can result in huge liabilities.

One source of potential liability is the contracts that the retailer makes with card issuers in order for the store to accept credit and debit cards as payment for transactions. Typically, these contracts require that merchants comply with PCI Data Security Standards. Failure to comply with the standards exposes a merchant to two types of liability. First, the contract with the card issuer provides for substantial penalties if the merchant does not comply with PCI standards. Second, and more significantly, merchants are subject to “push-back” liability for damages suffered by the card issuer as a result of the merchant’s data breach. These losses sustained by card issuers include not only the fraudulent charges made on the accounts of the victims of identity theft, but also the administrative costs associated with the issuance of new cards to customers whose personal information may have been compromised. For TJX, the bulk of its liability will likely result from such push-back losses sustained by issuers.

Another source of risk to retailers is the growing number of state laws regarding notification of security breaches. According to the National Conference of State Legislatures “State Security Breach Notification Laws” webpage (www.ncsl.org/programs/lis/cip/priv/breachlaws.htm), as of May 1, 2008, at least 42 states, the District of Columbia, and Puerto Rico have legislation requiring notification of security breaches involving personal information.

The New York statute (New York State General Business Law section 899-aa, subsections 1 and 3) is fairly typical. It applies to any New York businesses that own, license, or maintain computerized data containing “private information,” such as an individual’s Social Security number, driver’s license number, or account number, along with the required access code or password needed to permit access to an individual’s financial account. These businesses must notify any New York resident whose private information was acquired, or believed to have been acquired, by someone without valid authorization. If the business fails to promptly notify the affected parties, the statute authorizes damages for actual costs or losses, including “consequential financial losses” [New York State General Business Law section 899-aa, subsection 3(a)].

What Auditors Can Learn from the TJX Fiasco

When evaluating the risks associated with a retailer’s business, valuable lessons can be learned from the mistakes of TJX. Although TJX is a huge organization, these risks are equally applicable to mom-and-pop operations. [Exhibit 1](#) summarizes these lessons.

First, check to see if there is wireless access to the company network. Even if company policy prohibits wireless routers, a renegade router installed by an employee may be connected. If wireless access does exist, evaluate the type of encryption used by the router. Make sure that a method prescribed by PCI standards, such as WPA or WPA2, is in use. Under no circumstances should WEP encryption be used. In addition, evaluate the strength of the log-on password and make sure that the router doesn’t broadcast its network name or service set identifier (SSID). Where practical, the authors recommend

configuring the router to restrict access to specific computers, using the unique media access control (MAC) address assigned to each authorized computer.

Second, evaluate the company's data storage practices and security for stored customer data. Ascertain that the company complies with PCI security standards and is not retaining excess data scanned from customer credit and debit cards. Under no circumstances should a merchant retain a customer's debit card PIN. Also, make sure that customer data stored by the retailer are encrypted using a strong key.

Finally, review the company's data-retention policies and practices. Make sure the merchant does not retain customer data any longer than permitted by the card issuers. Even better, do not retain data any longer than necessary to document the underlying transaction. Ensure that policies are in place to notify customers of possible security breaches and that a process is in place to implement the policies if a breach occurs.

Ultimately, the security of a company's information system relies upon the competency and honesty of its employees. Therefore, it is important to conduct background checks on employees and to train them about the possibility of security breaches and how to avoid them.

Gary G. Berg, PhD, CPA, is an associate professor of accountancy at East Tennessee State University, Johnson City, Tenn.
Michelle S. Freeman, EdD, CPA (inactive), is an assistant professor of business administration at Tusculum College, Greeneville, Tenn.
Kent N. Schneider, JD, CPA, is a professor of accountancy, also at East Tennessee State University, Johnson City, Tenn.