

The Importance of Data Security

by Kelley Damore, Editorial Director, TechTarget Security Media

The recent TJX data breach serves as an important reminder of how critical strong information security is within an organization.

In late January, TJX Companies officials disclosed that an attacker exploited a flaw in a portion of TJX's computer network that handles customer credit card, debit card, check, and merchandise return transactions. By March, they disclosed to the SEC that 45.7 million credit and debit card numbers were stolen over an 18-month period. Personally, I have been issued two new bank cards as a result of the TJX breach. Chances are you or someone you know has also been notified and is at risk.

The cost to TJX will be huge. When an organization suffers a data breach the Ponemon Institute, a leader in independent research on responsible information management, says it costs \$182 per lost record to notify victims, as mandated by law in 35 states. This figure includes legal fees, call center costs, notification letters, credit reports and lost productivity. Others estimate this breach alone will cost the retailer \$1.6 billion dollars. This dollar amount does not include shareholder lawsuits, regulatory fines or costs associated with bad PR or a tarnished brand image which are harder to quantify but potentially even more damaging over the long term.

In response to highly publicized data breaches such as this and others where laptops or backup tapes were stolen or misplaced, organizations are taking a much closer look at data protection in 2007.

In fact, according to a recent *Information Security* magazine/SearchSecurity.com survey of more than 608 enterprise security professionals, 80% of enterprises say protecting data is more important in 2007 than last year, and 72% admit they need a better strategy. As a result we're seeing renewed interest in encryption and new emerging product sets designed to address security needs.

While encryption technology has been around for quite some time, advancements in practical cryptography make data encryption more user-friendly and easier to implement and manage across multiple applications. The Federal government is leading the way on this front by mandating all government-owned laptops and mobile devices have their entire hard drives encrypted. As a result, full-disk encryption, mobile device and backup encryption markets are picking up speed.

Meanwhile, databases are most often a company's most important technology asset. Database security is another technology that is becoming very important. This involves encrypting fields of data within a database, running vulnerability scans against the database and monitoring database traffic for exploits and anomalies.

Finally, some other companies such as Microsoft and Adobe are taking a different approach. By putting the security controls on the document, organizations can restrict who has rights to the document and what a user can do with that document. This emerging market is called enterprise rights management or digital rights management.

Will data breaches end any time soon? I doubt it. But the good news is innovative companies and start-ups are offering technology that will help us get one step ahead of the bad guys.