

Securing Information is Smart Business

Written by:

Frank R. Mitchell, CITRMS

Thomas Glanville, CITRMS

Every business manages personal, financial, medical, or business information in one form or another. Confidential and Sensitive Information is necessary for most business operations. However, there can be serious consequences for the company owners, executives, employees, contractors, and consumers if that information is lost or stolen. The results of a breach are often imposed fines and penalties, loss of customers, and potential class action lawsuits involving those who become victims of identity theft.

Identity theft and fraud is growing at an alarming rate. As of January 11, 2008, the Privacy Rights Clearinghouse has documented that 217,393,476 records have been compromised from United States government agencies, businesses, schools, and other organizations since January 2005! According to a Javelin Strategy & Research Survey in February of 2007, the total one year amount of identity fraud in 2006 cost \$55.7 billion.

Most identity theft scrutiny in the public arena has concentrated on financial data loss, and of that, credit cards have been made the most visible. But businesses are less aware of non-financial data that is in their possession that is just as protected as credit card numbers. In fact, the concentration over the last few decades on credit card account theft has led to the Federal and State governments scrutinizing other forms of consumer data losses to build public awareness of the wide spectrum of identity theft as a whole. For any given business, if data is collected on personal, financial, business, and medical information on employees, customers, and contractors, and any of that data is lost or stolen, there are serious consequences for an unprepared company.

In addition to requirements imposed by state and federal legislation, perhaps the greatest impact to business is negative publicity and loss of trust among consumers. “If you experience a security breach, 20 percent of your affected customer base will no longer do business with you, 40 percent will consider ending the relationship, and 5 percent will be hiring lawyers!” (CIO Magazine, *The Coming Pandemic*, Michael Freidenberg, May 15th, 2006).

In the event of a loss or breach, there can be “safe harbor” for businesses that make a reasonable effort to safeguard Confidential and Sensitive Information. This includes the designation of an information security officer, creating and implementing policy, and training employees. As they say, “an ounce of prevention can save a pound of heartache.”

Identity Theft LOSS Prevention, LLC is a risk management firm dedicated to helping businesses make a reasonable effort to safeguard information and to reducing the probability of security incidents. For more information please call 888-LOST MY ID.