Published on *The National Law Review* https://natlawreview.com

Businesses at Risk: Protecting Your Valuable Data (Part 1)

Article By:

Neil B. Posner

Companies rely on a variety of methods to maintain the security of their property. Video cameras and identification badges are used to monitor the premises and control access to buildings and restricted areas. In a retail setting, merchandise sensors help prevent theft. Certain organizations take a more extreme approach to security, including the use of eye scanners and fingerprint/voice recognition equipment. All of these measures are intended to protect a company's property, plant, personnel and intellectual property.

But what methods are used to maintain the confidentiality of sensitive data and other valuable information (e.g., personal health information and financial data)? We are all familiar with passwords that are required to log on to computers or access certain online resources. But is password protection enough? In today's world of computer hackers and identity thieves, statutes and regulations are passed every year that govern data privacy and information protection. Failure to comply can be costly and potentially devastating for businesses of every shape and size.

It Happened to Them

Recent real-life examples underscore the significant risks. In late January of 2010, BlueCross BlueShield of Tennessee reported that the October 2009 theft of computer hard drives containing personal information on hundreds of thousands of its members had already cost the insurance company more than $7 million. These costs, however, are minimal compared to what TJX Companies (parent of Marshalls, T.J. Maxx, HomeGoods and several other discount retail entities) had to pay for a breach of its systems.

In 2007, TJX announced that its computer systems had been hacked and that the credit and debit card information for more than 45 million cardholders had been accessed over an 18-month period. However, the banks associated with the stolen information alleged that the number of cardholders affected was actually closer to 94 million. The breach resulted in numerous lawsuits, including those involving the affected banks, credit card companies and representatives of consumer class actions. In addition, numerous states sued TJX alleging that the company ignored flaws in the configuration of its computer network and failed to take sufficient steps to protect customer information. In response, TJX set up a $107 million reserve to fund the costs associated with the lawsuits and settlements. According to some estimates, the TJX breach, including fixes to the company's information systems, has already cost the various parties involved more than $250 million.

Government Reacts with New Legislation

The federal government and numerous states have imposed tougher restrictions on the security and disclosure of data and personal information. Prior to the TJX breach, health care providers were already subject to the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA has provisions that govern the privacy and security of information, including protected health information (PHI), a key term that is very broadly defined. More recently, however, the American Recovery and Reinvestment Act of 2009 made several significant changes to HIPAA through the Health Information Technology for Economic and Clinical Health Act, also known as the HITECH Act. Many of its provisions became effective in February 2010.

In addition, the Federal Trade Commission (FTC) recently established the Red Flags Rules, which require financial institutions and creditors to develop and implement written policies to prevent identity theft. These policies must identify, detect and respond to practices or specific activities that could indicate identity theft. In an attempt to determine whether certain organizations and professions are subject to the provisions of the Red Flags Rules, numerous lawsuits have already been filed and are winding their way through the courts. Although the FTC has delayed implementation of the Red Flags Rules several times, they are currently set to go into effect on June 1, 2010.

Another area of concern involves the personal financial information of consumers. Information of this sort that is held by financial institutions is subject to the Financial Modernization Act of 1999. Also known as the Gramm-Leach-Bliley Act, this legislation gives authority to eight federal agencies and the individual states to administer and enforce the regulations contained in the act. Even though the act applies specifically to financial institutions, that category is broadly defined to encompass banks, securities firms, insurance companies and entities that provide financial products and services to consumers.

In addition to the federal statutes and regulations already mentioned, some states have passed their own laws dealing with notification to consumers whose personal information has been acquired by an unauthorized individual.

It Can Happen to You

The important thing to remember is that virtually every business is at risk. Over the next two issues of the *Litigation & Counseling Alert*, we will explore data privacy and security in more detail, including an in-depth discussion of the HITECH Act, the Red Flags Rules, the Gramm-Leach-Bliley Act and various state statutes, as well as how this legislation can affect your business. In addition, we will address several ways that companies can use contractual provisions to reduce their risks regarding data security and privacy. Finally, we also will discuss the availability of insurance to cover data theft and privacy breaches, along with the important questions to ask your insurance brokers and legal advisors.

Editor's Note: This article is the first in a series that will highlight some of the substantial risks associated with the loss of sensitive data and summarize ways you can help protect your organization.

National Law Review, Volume , Number 88