Massachusetts Data Protection Regulation

ezTechDirect

A First in Data Security Law

The nation's most stringent data security law, the Massachusetts Data Protection Regulation (MA 201 CMR 17), is now in effect. For the first time ever, a government body has mandated the use of a specific technology to enforce privacy regulations. Massachusetts (along with Nevada, which passed a similar law) requires that businesses encrypt all the transmitted, personally identifiable information (PII) of their customers.

Not only does this law apply to Massachusetts businesses; it applies to any firm conducting business with a resident of Massachusetts, including third-party vendors. In effect, a company who wants to sell anything to a resident of the nation's 13th largest economy must adopt these measures.

Largest Data Breach in History

These regulations were enacted as a result of the most significant data breach in history. In 2007, TJX Companies, based in Framingham, Mass., announced a data breach in which hackers exposed at least 45.7 million credit and debit card holders to identity fraud.

After settling a number of lawsuits, TJX has agreed to implement tighter security and obtain independent audits every other year for 20 years, according to a settlement reached with the Federal Trade Commission.

As a result of this catastrophic data loss, this law was designed to protect consumers on three fronts:

- To insure the security and confidentiality of customer information
- To protect against anticipated threats or hazards to the security or integrity of such information
- To protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer

Beyond Encryption

The Massachusetts law is much more than an encryption mandate. Encryption is only a part of an overall information security plan that businesses must develop. Other computer system requirements include: secure user authentication protocols, secure access control measures, reasonable monitoring of systems, and up-to-date software.

Beyond system requirements, businesses are also accountable for making sure that their human resources can implement and maintain these programs. A business must: 1) designate one or more employees to maintain the security program, 2) provide ongoing employee training, and 3) develop security policies for employees relating to the storage, access, and transportation of records.

However, according to the Commonwealth, these safeguards should be appropriate to the size of the business, the amount of resources available to that business, and the amount of sensitive data stored. Essentially, the law requires businesses to put forth a "best effort" to ensure certain types of data are protected.

If a public data breach does occur, the application of this law will hinge on the answer to the question, "Did you do everything within your power to protect this information?" To some extent, this nebulous definition can lead to legal debates of technical possibilities versus financial burden.

Businesses Are Culpable for Third Parties

Businesses are also culpable for the security practices of any third-party vendors that may have access to the personally identifiable information of their clients. Companies must take "reasonable steps" to select third-party service providers that maintain appropriate security measures.

Even before data is transported to our mirrored data centers, it is encrypted using 256-bit AES security—a more stringent level of security than even online banking institutions use. Our data centers—located thousands of miles apart—have biometric controlled access, 24/7 monitoring, and backup generators.

The Bottom Line

Though Massachusetts and Nevada are the first states to enact these strict data laws, the rest of the country is not too far behind. California—the largest state economy in the United States—has enacted a notification law as has Virginia, Iowa, and South Carolina among others. All businesses that handle personally identifiable information would be wise to prepare as if a national requirement was on the horizon. It makes good business sense to secure customers' data to the fullest extent, because companies that are proactive in protecting their customers will retain their loyalty.

ezTechDirect LLC • P.O. Box 1245 Camp Hill, PA 17001 • 717-602-1048 • www.ezTechDirect.com