Does Your Company Have An Information Security Program? Is it Up To Date?

The data breaches that Target, Michael's, Nieman Marcus and other large companies have suffered recently have gained a great deal of attention in the media. These public and costly embarrassments serve as reminders that all businesses should have a comprehensive information security policy and should closely monitor their servers and third party data interfaces for potential breaches.

Since 2010, Massachusetts has had one of the country's strictest data security laws. What many companies fail to realize, however, is that the Massachusetts rules apply to businesses located outside Massachusetts. Any business (wherever located) that has one or more employees or customers who live in Massachusetts is most likely subject to the Massachusetts data security requirements and is required to have an information security program. If pending federal legislation is passed, even more businesses will be required to adopt similar information security programs.

Currently, any person or business that owns, stores or maintains personal information about a Massachusetts resident is required to: (a) develop, implement and maintain a comprehensive, written information security program; (b) implement physical, administrative and extensive technical security controls, including the use of encryption; and (c) verify that any third party service providers that have access to this personal information can protect the information. "Personal information" can be as little as a first name, last name and the last 4 digits of a social security number, credit card number or bank account number of a Massachusetts resident.

There are several reasons why it is important that all businesses, even those not specifically covered by the Massachusetts data security requirements, prepare and update an information security policy:

- Information security policies help to reduce the risk of liability and adverse publicity should a data breach occur. The Massachusetts Attorney General has pursued and obtained six figure civil judgments for violations of the requirements.
- As mentioned above, any federal legislation that is passed is likely to be modeled in the Massachusetts requirements. Businesses not covered presently by the Massachusetts requirements should get a jump on their compliance obligations.
- Information security programs subject to the Massachusetts requirements must be reviewed at least annually. Many companies who initially prepared information security policies have not reviewed or updated their policies since 2010.

Date Created
March 15, 2014