**What Is MA 201 CMR 17?**

By, ***John J. DeMauro***, President, Practical Security Solutions, LLC

In September 2008, Massachusetts introduced what many say is the toughest data protection law in the country. Spurred by a number of high profile data security incidents, MA 201 CMR 17 is designed to prevent data breaches and identity theft. This law applies to businesses of any size and in any industry that own, license, store, or maintain personal information about a MA resident, as well as to any business that handles MA residents' personal data regardless of where that business is located.

The law, was initially set to take effect on January 1' 2009, but was extended to January 1, 2010 "in light of intervening economic circumstances", according to the State. After several public hearings and the implementation of certain changes suggested by business and information security advocates, the deadline was ultimately pushed back to March 1, 2010. Businesses only have a few months at this point to review and update their data security practices if they hope to achieve compliance with the new law.

If your business is in healthcare, financial services or any other industry that now complies with an existing data security regulation (i.e. HIPAA, GLBA, or PCI), good news - you have a head start on the new law. Businesses that handle significant amounts of personal data, such as CPA and law firms, that haven't implemented a robust information security program, will likely be impacted by the law the most. Small businesses will feel an impact due to their smaller budgets and their typical lack of in-house IT expertise.

The requirements for MA 201 CMR 17 are based on sound information security standards and are designed to protect personal data. The law requires that businesses develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing personal information. An important piece to remember as you prepare to comply with this new law is that it applies to paper documents as well as electronic information.

We recommend that you begin your compliance effort by performing a risk assessment to ensure that security controls are based on the specific data security risks inherent to your organization. Start by asking three questions. First, where is personal data located, who has access to it, and how is it used? Second, consider the various ways the data could be exposed and where the possible weaknesses in your security controls may lie. Finally, implement the controls necessary to reasonably protect your data.

Key risk management activities you should consider are:

- Reducing the amount of personal information you maintain to the minimum required to conduct business.
- Limiting both physical and logical access to only those that have a true business need.
- Monitoring computer event logs.
- Be proactive. Prepare for an incident before it happens. Be ready to react and know who to engage, as well as whom to notify and when.
- Building and maintaining security awareness throughout your organization. This is the most important element of your program and must be in place for all else to succeed.

We believe that businesses should go beyond just achieving compliance with 210 CMR 17 when they design their data security programs. They should make protecting critical and confidential information a business priority and create a "culture of protection" within their organizations. Implementing and maintaining a comprehensive data security program has become an essential business process that will help protect the long term viability of your business. The financial and reputational damage caused by a data breach could have a significant and lasting negative impact on your organization. Truly progressive businesses will likely recognize this as an opportunity to differentiate themselves from their competition and tout their compliance efforts.