



**BOSTON
TECHNOLOGY
ADVISORS, INC.**

The New Massachusetts Data Security Laws: What 201 CMR 17.00 Means to Your Business

Bob Berman, President, Boston Technology Advisors, Inc.

October 2, 2009

What is 201 CMR 17.00?

During the year 2008, the Massachusetts State Legislature passed item 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth, which will require all business which store or transfer the **personal information** of any Massachusetts Resident to comply with a new set of data security requirements.

Does this affect your business?

All business operating in Massachusetts must comply, regardless of size.

Personal Information is defined by the State as any combination of a persons name, social security number, financial account information, or credit/debit card number. If you store any of personal information, regardless of customer or employee data classification, then this new law pertains to you and you are expected to comply.

What does your business need to do to comply?

Meeting the new legal requirements can seem like a daunting task, but it can be broken down into just a few areas of focus that will allow all businesses to comply quickly and efficiently.

Taking Action

The new set of information protection can be broken down into three areas of focus; Assessment, Process, and People.

A. Assessment:

- Do your company's current data security practices meet the

62 Lanewood Ave.
Framingham, MA 01701
(508) 275-2011
(775) 535-1226 fax
www.bta-advisors.com

new requirements?

- What third parties have access to the personal information you are storing, are they in compliance?
- Do your current computer and networking systems comply with the new requirements?

B. Process:

- Create and document your company’s Security Program” policy.
- Create and communicate explicit agreements with third party vendors and partners to ensure that they are complying with the new requirements when dealing with your data
- Ensure that the Security Program is being monitored on a regular basis, including an in-depth annual review
- Ensure that access is immediately turned off for terminated employees
- Create a process for dealing with employees who do not comply with the new regulations

C. Implementation:

- Upgrade non-compliant systems and network components where necessary
- Make any third party vendor and partner changes needed in order to meet compliance
- Identify an employee to become the “owner” of the “Security Program”
- Train employees on the law and what it means to their day to day jobs

Conclusion:

Complying with 201 CMR 201.17 may seem like a daunting task, but overall the law makes sense from a data security perspective. It is important for a company to protect not just what the State of Massachusetts defines as Personal Information, but also any data that is important to an organization’s success. Not complying is both dangerous for your data and could result in steep fines from the State of Massachusetts if data is stolen from your ownership.

Boston Technology Advisors can help. We understand business, we understand technology, we understand security. Give Boston Technology Advisors a call at 508-275-2011 to setup a time to discuss the new laws, how they impact your business, and how we can help your business comply.