

Massachusetts' Data Security Regulations: Compliance in Five Easy Steps

Massachusetts now has arguably the broadest data security regulations in the country. These regulations – which cover businesses inside and outside of Massachusetts – require the development and implementation of a comprehensive and detailed information security program by May 1, 2009.

It is estimated that the compliance effort in Massachusetts alone will cost in excess of \$1 billion, with virtually every Massachusetts employer impacted. Satisfying the regulatory requirements is not simply a question of allocating resources, however. It demands a dedicated and well-planned effort.

1. Designate the right point person.

Every campaign needs a general; pick yours carefully. Compliance is not simply an IT concern. It involves risk management, legal and contractual issues, and HR responsibilities such as workforce education, discipline and training. Designate someone comfortable in all of these areas, with the authority and ability to implement organization-wide process and policy changes.

2. Pick your battle.

There are two distinct ways to attack the problem: protect “personal information” of Massachusetts residents only to the extent required by the regulations, or instead, use compliance as part of a broader effort to restructure your organization’s overall approach to data security, confidentiality and integrity. The minimalist option may, for example, counsel in favor of segregating “personal information” from other data, and focusing on systems and personnel having direct contact with such segregated information. Alternatively, the broader approach may impose changes across the organization regarding the way computer systems are used and information is treated generally.

The correct choice may not be obvious and will depend on your business’ circumstances and resources, but it should be made early in the process to avoid a waste of those resources later on.

3. Assess your organization’s status early.

Assess the current state of affairs. What kind of sensitive personal data is maintained by your business? (It will often fall into three categories: HR information about your employees, customers’ credit card and other payment information, and personal information from customers used in the actual operation of your business.) What structures, if any, are in place to dictate how information is treated? How can strengths be leveraged? What areas will require fortification first? An assessment will determine where resources need to be concentrated, and help identify stakeholders to include early in the process. A successful battle plan is not developed in the abstract; it must take into account the readiness and resources of the units involved in its implementation.

4. Don’t operate in a vacuum.

Communicate. With other similarly situated companies. With your IT service providers. With your legal counsel. These regulations are new and unlike anything seen before. Don’t expect to just “know” how individual provisions will be interpreted or enforced by the state, or what software and hardware products are best suited to satisfying their requirements, or what contractual language will provide you with the best protection when dealing with insurers, customers, or service providers. Gather intelligence.

5. Take a step back.

Merely completing a checklist may provide a false sense of security. In the event of a data breach, the Attorney General will not be the only one knocking at your door. Expect plaintiffs’ lawyers, insurers, and contract partners to all question your regulatory compliance. To manage and mitigate exposure, perform a risk assessment **after** completion of your written security plan and **before** a data breach can occur.

If you would like more information on this topic, please contact the head of the firm’s Data Security Practice Group, Joe Laferrera, at joe.laferrera@gesmer.com.

This information is provided “as is.” No representations are made regarding completeness, accuracy or applicability. It does not constitute legal advice and creates no attorney-client relationship. This may be deemed advertising under M.R.P.C. 7.3(c). All rights reserved. ©2008 Gesmer Updegrove LLP.