

Executive Summary

Compliance with Massachusetts Data Security Regulations

*Survey distributed and results compiled and analyzed jointly by
Goodwin Procter LLP and the International Association of Privacy Professionals*

Over 200 people responded to this informal survey of the IAPP members and subscribers. The survey was conducted in the second half of August 2009 - starting the same day as the recent amendment to the regulations on August 17, 2009. For various reasons, the survey is not necessarily representative, and has not been normalized to account for such factors. For instance, the respondents are members or otherwise connected to the IAPP, and thus may not be representative. Additionally, the self-selection bias in choosing to respond to such a survey also may cause skew. Moreover, sometimes the respondents did not know the answer on behalf of their organization.

The respondents identified themselves as from 27 different states and the District of Columbia. Massachusetts had the largest representation with 18% (and thus 82% of respondents did not identify as from Massachusetts). Other states with over 5% of the respondents were California, Florida, Illinois, Minnesota, New York, and Ohio. The survey included organizations with fewer than 1,000 employees (19%) and greater than 10,000 employees (50%). 70% of the organizations who responded have an annual revenue of more than \$100 million.

As far as type of business, 16% of organizations defined themselves as Financial – Banking, and 15% as Technology. Other categories with over 5% of respondents were Healthcare (9%), Retail (8%), and Professional Services (5%); while fewer than five percent of respondents were in Financial – Mutual or Private Fund (4%), Industrial (3%), or Hospitality (1%), or Telecommunications (0%). The largest category of respondents categorized themselves as “Other.” (38%).

Some significant findings from the survey are as follows:

Awareness of Rules and Scope of Rules:

- 91% were aware of that Massachusetts had enacted comprehensive data security rules.
- 88% were aware that the Massachusetts rules protect personal information of Massachusetts residents, even if their organization is not located in Massachusetts.

Scope of Compliance: Identifying records, training employees, and vendors

- 76% of organizations maintain personal information on Massachusetts residents.
- 39% of organizations had identified all records used to store personal information of Massachusetts residents, and 31% were in the process of doing so.

- 20% had not identified all records used to store personal information of Massachusetts residents.
- 25% of organizations had provided information or training to employees on the Massachusetts rules, and 32% were in the process of doing so.
- 34% had not provided information or training to employees on the Massachusetts rules.
- 51% of organizations had identified third-party providers (vendors) who have access to personal information, and 36% were in the process of doing so.
- 60% have over 10 vendors with access to personal information
- 30% have over 100 vendors with access to personal information
- For vendors, 33% of responding organizations require a written certification of compliance, and 24% require a response to a questionnaire. 8% conduct an audit.

Expenditures Made to Comply with Rules:

- 33% of organizations spent more than \$50,000 on complying with the rules.
- 12% of organizations spent \$10,000-50,000 complying with the rules
- 44% of organizations have spent more than 100 hours on complying with the rules.
- 17% of organizations have spent 40-100 hours complying with the rules
- About 17% of organizations have engaged a consultant or a law firm to assist with compliance, and about 77% have not.

Compliance with Rules:

- Across a broad set of compliance factors, approximately 60% (53-66%) of organizations responded that they had completed each factor, and approximately 28% (23-35%) were in the process of doing so. The compliance factors specifically requested (and the percentage complete) were:
 - analyzing internal and external risks to personal information (66%);
 - encrypting all personal information on laptops (64%);
 - implementing a “comprehensive, written, Information Security Program” as required by the Massachusetts rules (60%);
 - developed a written policy for the safekeeping and transport of, and access to, personal information at off-site locations (58%);
 - encrypting all wireless networks (57%);
 - and implementing or improving safeguards for personal information (53%).
- 40% of organizations rated themselves as 81-100% complete with their compliance efforts with the rules to date.
- 25% of organizations rated themselves as 61-80% complete with their compliance efforts with the rules to date.
- 60% of organizations expect compliance efforts to be complete by March 1, 2010.
- 29% of organizations expect compliance efforts to be “probably” complete by March 1, 2010.