Interpreting 'risk' in the Massachusetts data protection law
by David Navetta, Esq., CIPP

By now, most information security professionals, and at least some lawyers, are aware of the Massachusetts data protection law (201 CMR 17.00), which legally establishes standards for the protection of state residents' personal information. The regulation, after multiple previous "final" versions within 11 months, is one of the first attempts by a state to impose detailed information security requirements for "both paper and electronic records" across a wide and diverse swath of the business community. The revisions and general confusion surrounding the guidelines are an indication of the difficulties regulating in this area.

The law attempts to achieve its purpose by requiring two general activities of companies that "own or license" personal Information:

(1) The establishment of a written information security program (201 CMR 17.03).

(2) The implementation of specific computer system security controls (201 CMR 17.04).

The regulation varies significantly from other laws that, rather than requiring specific controls, more generally require the implementation of "appropriate," (e.g. "GLBA") "reasonable" (e.g. Cal AB 1950) or "adequate" (e.g. "SOX") information security controls. In an attempt to assuage angry small-business owners, the latest version of the Massachusetts data protection law utilizes a "risk-based" approach and mandates specific requirements and controls. As such, one could say the regulation represents a hybrid approach: Specific controls and policies are required, but those requirements are tempered by the amount of risk an entity poses. The question for security pros and lawyers is: What does this mean in practice?

One of the key practical issues is how to interpret the regulation's "risk-based" language, and how to apply it to an organization's particular set of circumstances. This is ultimately a legal question, making it extremely important for a company's security team to engage its legal team when developing a compliance plan. Without legal training, it will be difficult for security professionals to know how the courts, regulators and potential plaintiff's attorneys will interpret and apply the regulation. Let's look at key risk-based aspects of the regulation that your compliance and legal teams will need to be prepared for.

Interpreting risk-based language

The Massachusetts data protection law provides little guidance on how to interpret and apply its risk-based terms. This exercise is complex because interpretations may vary, and the application of these factors may differ from one organization to the next. The following legal issues demonstrate the difficulty in applying the risk-based language:

- **How should organizations weigh the risk-based factors?** Size, resources and the amount of stored data can all be considered in determining the amount of risk a company poses. If a company is small and without resources, but has a lot of stored personal information, what is the more important "risk" factor: the size of the company, or the volume of data? The regulation does not say, and this is where significant legal analysis and positioning are required.

- **Assuming a company is "lower risk," how does that affect the requirements of the mandated written information security program?** One might take the position that some (or even most) of the written information security program requirements do not have to be in place at all. If an organization carries a "lower risk," it may decide the written information security requirements do not have to be as detailed or deep. For example, 17:03(f) requires the documented security program to contain provisions mandating "reasonable steps to select and retain third-party service providers." These types of activities can range from doing a full-blown security assessment of a service provider to obtaining a written letter from the provider whereby it acknowledges that it has reasonable practices in place. For lesser risk organizations, the latter may be appropriate. Again, the regulation does not specifically indicate how the program requirements should be applied.

- **When is the maintenance of a security control not "technically feasible?"** Organizations do not need to maintain the controls listed in 17:04 if it is not "technically feasible" to do so. One problem with the term is that it focuses on technical aspects rather than "cost feasibility" or "business feasibility." A regulator or plaintiff's attorney could argue that practically anything is technically feasible without taking price into account or potential disruptions or problems with business practices and activities. Unlike the risk-based factors for the written information security in 17:03, the regulation does not explicitly reference the "resources available" to the company as one of the factors for determining whether something is "technically feasible." Again, organizations must stake out careful legal positions and anticipate potential counter-arguments before relying heavily on the "technical feasibility" limitation of the regulation.

Resolving the ambiguities of "risk"

Before an enterprise begins to craft its compliance strategy, it should establish attorney-client privilege with in-house or outside counsel in order to establish confidential communications between the legal team and security professionals working on compliance. While not foolproof, and sometimes subject to erosion in court, the attorney-client privilege may allow the organization to prevent certain communications between legal and security concerning compliance from getting into court. For example, let's say a company is sued and the issue is whether its written information security program was robust enough to comply with the Massachusetts's regulation. Legal discussions between the attorney and security pro concerning the decision to go with a less robust written information security program might not be accessible by the plaintiff's attorney that sued, and would not get in front of a jury or judge. This could significantly lower the company's risk of being found liable.

Ultimately, if a company chooses to do what some may interpret as less than the regulation strictly requires, it must develop a security-based rationale for the decision and use that to craft a legal position explaining why -- based on the risk-based factors in the law -- the company poses less risk and need not have the most rigorous controls. Years later (sometimes after key personnel have moved on), in the event a breach occurs and its compliance with 201 CMR 17.00 is called into question, this documentation can assist the organization in establishing that it was in compliance, and it will serve as the basis of any defense should one be necessary.

Generally speaking, a 201 CMR 17.00 compliance exercise should be thought of more in terms of developing a defensible legal position. Nonetheless, in most cases a solid security foundation, combined with an in-

depth compliance analysis, will yield the best results for the organization from an operational and legal standpoint.

Compliance with any law is a difficult process, and it is made even more difficult when dealing with a complex subject matter such as information security. For laws like the Massachusetts regulation (as well as a host of others, including GLBA, HIPAA, the EU Data Protection Directive and Nevada's Security of Personal Information Law), it is more important than ever for attorneys and security professionals to work together. These professionals must come up with a shared understanding of the risk their organizations are subject to, and jointly develop a plan that reduces the risk to an acceptable level and satisfies the specific criteria of these "risk-based" laws. A failure to do so can get a company into severe legal trouble.