BROOKS PIERCE

# What's So Great About an Information Security Policy?

09.28.2015

Lawyers and compliance professionals constantly tout the importance of internal information security policies, particularly in light of data privacy problems that are reported almost daily in the media. Admittedly, drafting such policies as a proactive measure can be a pain because there is always a tendency to worry that, unless you've suffered a data breach, you are the proverbial "solution in search of a problem."

But it's not. In fact, in some cases, it's actually required. HIPAA (for protected health information), Gramm-Leach-Bliley (for financial information) and Regulation S-P (for broker-dealers and investment advisors) have specific federal rules related to information security practices and policies. However, it would be unwise for a company that isn't covered by these industry-specific rules to think a security policy isn't needed.

It's nearly inevitable that your company will suffer some sort of data incident in its corporate life cycle. Even if not required, an information security policy can provide companies with important real-world benefits when responding to a data security incident.

First, the information security policy can be used as a benchmark for training employees on data security and, just as importantly, data breach response. A good security policy will include, at a minimum, information about (i) how personally identifiable information will be collected, stored and shared, (ii) how to report a possible data security incident, (iii) how users/customers will be notified of an incident, and (iv) the appropriate "point" persons in the company responsible for handling data privacy incidents.

Second, your company's insurers, auditors, clients or customers may well require that you have an information security policy in order to demonstrate a competence in data privacy. Being able to report affirmatively that you have a policy – as opposed to saying you "will prepare one" – showcases that your company is a privacy-forward company. In the event of a breach, regulators or litigants could potentially raise questions about your data security practices. The fact that you have an information security policy that you implemented both before, during, and after the breach helps show that your company took commercially reasonably steps to secure the information breached.

Speaking of data breaches, an information security policy also has a back-end benefit both to the company and its users. For companies that provide products or services online, a user's e-mail address is often the one and only way to communicate with the user in the event of a data breach. Yet many state laws do not allow for e-mail notification unless the company has obtained the prior consents required under the federal E-Sign Act (which few online companies likely can achieve a as a practical matter). But many states have provisions that allow companies with existing information security policies to follow the data breach notification procedures contained within their IT security policy. If applicable, these provisions can allow companies to notify their users electronically. This provides a more cost-effective approach to notice in large breaches and often reflects the most practical method of communicating with the company's users or customers.

Of course, an effective IT security policy must be put into practice – a "living" document that is part of your company's privacy culture. The mere exercise of preparing an information security policy will bring your key employees together to thoughtfully consider your current practices and revise them to become best practices on both the front end and the back end of a data breach.