Does Your Company Have a WISP? Have You Updated It Lately?

By Colin A. Coleman, John E. Ottaviani, or Brian Reilly

Does your business have employees or customers in Massachusetts or Rhode Island? If so, you need to have a written information security program ("WISP").

If your business (wherever located) collects, stores or uses personal information about a Massachusetts resident, you are legally required to: (a) develop, implement and maintain a comprehensive WISP; (b) implement physical, administrative and extensive technical security controls, including the use of encryption; and (c) verify that any third party service providers that have access to this personal information can protect the information. "Personal information" can be as little as a first name, last name and the last 4 digits of a social security number, credit card number or bank account number of a resident. We note that the requirements under current Rhode Island law are similar to those under Massachusetts law, but not quite as stringent. Because most Rhode Island businesses are likely to have employees or customers from Massachusetts, we advise that they comply with the more comprehensive Massachusetts requirements.

Business leaders need to understand that the WISP is a "program," not a "policy." The WISP is intended to describe a system by which one runs the business on a day-to-day basis to safeguard sensitive information. Our experience with WISP's is that some clients treat them like policies that they can have drafted and then throw in a drawer and never look at again. Some businesses have copied a WISP from a form found on the Internet, or a form provided by another company, but have not taken the time to customize it for their business. Other companies want to say they have a WISP, but do not actually make any operational changes to implement the purported security programs described in the WISP. Recent amendments to Massachusetts law make these practices, as well as not having a WISP at all, much more risky.

There are several reasons why it is important that all Massachusetts and Rhode Island businesses prepare an information security program and update it regularly:

- WISP's help to reduce the risk of liability and adverse publicity should a data breach occur. The Massachusetts Attorney General has pursued and obtained six figure civil judgments for violations of these regulations. In addition, the recent amendments to this Massachusetts law require breach notices to state whether or not the company maintains a WISP.
- Organizations subject to the Massachusetts requirements must review their WISP's at least annually. Many companies who initially prepared information security programs have not reviewed or updated their policies since 2010.
- Information security programs help with training employees in Company policies and procedures with respect to confidential and sensitive information.

If your company does not have a WISP, or if your company has not updated its WISP recently, or if your company's operations do not follow the policies and procedures set forth in your company's WISP, we would be happy to discuss these programs with you and assist with your compliance obligations. Please contact Colin A. Coleman, John E. Ottaviani, or Brian Reilly at Partridge Snow & Hahn LLP.

Date Created
March 6, 2019