Bringing Your Business Online: Written Information Security Programs (WISPs)

Description

The current COVID-19 pandemic has forced many businesses online in order to survive. In many cases, businesses had no plans to be online. Others were forced to move online more quickly than planned. In order to assist these businesses, we are preparing a series of articles discussing some of the more important legal issues to address when moving your business online. Article 1: Website Terms discussed online terms and conditions to protect your business. Article 2: Privacy Policy discussed how your business collects, uses and discloses personal information of others. Article 3: Third Party Content discussed the risks of copying photos, music, videos, and other content created by third parties onto your website. Article 4: E-Commerce Policies discussed e-commerce policies that a website selling products or services should have in place. Article 5: Creating Enforceable Contracts discussed the safest method to ensure that you can enforce your online terms and conditions protecting your business.

Article 6: Written Information Security Programs (WISPs)

In the context of an online business, a WISP is not a small bunch of hay or straw. If your business has employees or customers in Massachusetts or Rhode Island, you must have a written information security program (WISP). Many other states have similar requirements.

If your business (wherever located) collects, stores or uses personal information about an individual, many states have laws that legally require you 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 a first name, last name and the last 4 digits of a social security number, credit card number or bank account number of a customer.

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. This practice can be risky under state laws such as Massachusetts.

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

- WISPs help to reduce the risk of liability and adverse publicity should a data breach occur. State enforcement officials have pursued and obtained six figure civil judgments for violations of these regulations. In addition, the laws in some states require breach notices to state whether or not the company maintains a WISP;
- Some state laws, such as those in Massachusetts, require businesses to review their WISP’s at least annually. We see many companies who initially prepared information security programs but have not reviewed or updated their policies on a regular basis;

- 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 your requirements and assist you. Partridge Snow & Hahn Partner John Ottaviani has over 25 years of experience bringing businesses online and can provide the guidance needed to make the transition as painless as possible. He can be reached at jottaviani@psh.com or 401-861-8253.

Date Created
May 19, 2020