PortsmouthHerald

United States: Protect Your Customers' And Employees' Personal Information

December 2012
by Neil Nicholson

A Business Imperative for 2013

The protection of your customers' and employees' personal information remains a top priority to, well, your customers and employees. Therefore, it is more than just a good business practice to protect personal this information – it really is a necessity. To help you tackle this necessity in the first 14 days of 2013, use this ten step data security guide to develop a plan to protect Personal Information ("PI").

1. **Create a Data Security Team**. The Data Security Team should be comprised of human resource staff, accounting staff, divisional supervisors, and information technology experts. The team must have one person designated as the Data Security Coordinator who is responsible for the overall development, implementation, maintenance, and monitoring of a Data Security Program.

2. **Understand the Scope**. PI laws and regulations vary depending on your business industry and the geographical reach of your company. A certified public accountant, for example, with clients in all of New England will have to comply with federal regulations and state law and regulations from all New England states, while a construction company in New Hampshire may only have to focus on New Hampshire law if all its employees and customers reside in New Hampshire.

3. **Conduct an Assessment**. The definition of PI varies depending on the type of your business and application of state and federal law. Generally, however, PI is defined as an individual's first and last name or first initial and last name in combination with one or more of the following: Social Security number; driver's license number or government issued identification card number; financial account number or credit card/debit card number, with or without any required security code, access code, personal identification number, or password to access the account.

The assessment must address how your business accesses, uses, stores and disposes of PI. Answer the following questions: (1) How is PI acquired? Does it come in by regular mail, email, fax, employment applications, purchase orders, or invoices? (2) How is PI stored? Is it stored in file cabinets, desk drawers, staff offices, off-site locations, servers, laptops, workstations, photocopy machines, portable electronic devices? (3) How is PI used? Think about the people, processes and systems involved that have access to and use the PI. (4) How is PI shared with others within and outside the company? Does it get distributed by courier, email, regular mail, outgoing fax, and in what format? (5) How is PI destroyed when no longer needed? Document retention and collection policy, on-site or off-site shredding and disposal, electronic data disposal?

4. **Create the Data Security Program**. Use this outline as a guide, but consider seeking counsel to ensure your Data Security Program complies with the applicable state and federal regulatory schemes covering your company's industry.

5. **Train your Employees**. Like any other policy, your employees are better at meeting expectations when they know the expectations.

6. **Enforcement**. Develop procedures to address violations of the Data Security Program and make the PI protection expectations clear in the personnel plan.

7. **Third Party Vendors**. Take reasonable steps to verify your third party vendors have the capacity to protect PI and ensure through contractual means that the PI protection will occur.

8. **Implement Need to Know Strategy**. Restrict access to those individuals that actually need to know the PI to complete their job-related tasks. A need to know strategy includes developing confidentiality agreements with employees and a plan to immediately cut-off access to PI from a departed employee or independent contractor.

9. **Build a Breach Notification Plan**. Just like a fire evacuation plan, you hope you never have to use it and are thankful for the plan when used. Use a rapid deployment team trained to handle public relations logistics and deadlines of notification under applicable laws. As part of the plan, include a post-incident review, summary, and corrective action measures.

10. **Review the Data Security Program**. The Data Security Program should be evaluated at least semi-annually or whenever there are changes to the business model that could impact the protection of PI. Consider a mock test to evaluate its effectiveness.

Neil B. Nicholson is an attorney at McLane Law Firm licensed in New Hampshire and Massachusetts.

The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.