Cyber Preparation Moves to Main Street

As in *The Anchor,* First Quarter 2016

Is your organization prepared for a cyber-attack? No, this is not a tagline to promote or sell cyber security insurance (although the cyber-related insurance market is growing into the multiple of billions of dollars). It is a question for you and your customers. Increasing cyber threats and government regulations designed to protect against them, mean you should be looking to advise your customers on cyber security protection and assessing your agency's systems as to whether or not you are properly prepared for a cyber-attack.

Since 2008, ad nauseam, we have heard about those institutions that are "too big to fail." These national behemoths are so large with so much information that no one doubts their attraction for hackers. So, for example, when a Target (no pun intended) or Home Depot is the victim of a cyber-attack, we are not surprised.

But we can no longer bury our heads in the sand thinking we are too small to be a target. You and your customers must be prepared for when an attack occurs, not if one should occur. Additionally, new laws requiring systems to protect against data breaches require virtually all businesses to act.

There are many cyber-related insurance products available in the industry. But cyber insurance can only replace financial loss. While guarding against financial loss is a priority for you and your customers, it is not the only one. You must also consider damage done to your reputation and corporate integrity. Additionally, the potential that bodily and physical harm could arise from a cyber-attack is as of yet unknown. There are also third-party damages related to your preparation (or lack thereof) to encounter a cyber-attack. In other words, there are countless ways that liability could arise from having a substandard cyber-security system or worse having none at all.

States and federal agencies have been trying to get out in front of cyber-related threats and responses. For example, the NAIC has issued *Principles for Effective Cybersecurity: Insurance Regulatory Guidance*. The list of 12 principles obligates regulators to insure that they, themselves, as well as the insurers, producers, and other entities they regulate, protect personally identifiable consumer information. Similar obligations are imposed on financial institutions by federal regulators. Many states also have passed data breach notification laws.

During the 2015 legislative session, the Rhode Island General Assembly enacted the "Rhode Island Identity Theft Protection Act of 2015," R.I. Gen. Laws § 11-49.3-1, *et seq.* Effective in July 2016, this law requires any municipal agency, state agency, or "person" (which includes individuals and businesses of all sizes) that "stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident" to "implement and maintain a risk-based information security program," R.I. Gen. Laws § 11-49.3-2(a). The new law also prohibits any person from retaining personal information for longer than is reasonably required to perform the services requested, requires the destruction of all personal information in a secure manner (such as by shredding, pulverizing, incinerating or erasing), and requires that security measures be undertaken by third parties when personal information is shared. This statute also sets forth a procedure for notifying the attorney general and those affected by a security breach. R.I. Gen. Laws § 11-49.3-4. Reckless violations of this statute could result in civil penalties of not more than $100 per record while those violations adjudged to be willful could result in civil penalties of not more than $200 per record.

Still think your organization may not be impacted? If your agency maintains non-encrypted or hard copy paper format of an individual's first name or first initial and last name combined with a social security number, driver's license number account, credit or debit card number, medical or health insurance information, or email address with any required password granting access to an individual's personal, medical, insurance or financial account, then you have "personal information" subject to this statute. Virtually every business maintains this

information about its employees, and many have similar information about customers or clients. Also, if your agency suffers a data breach and you have customers in a different state, then you must comply with the notification laws of that customer's state. These laws are in conjunction with or in addition to the various federal laws dealing with industry-specific data security and privacy regulations.

Planning for and instituting a security and notification program is not a one-size fits all proposition. If you happen to be regulated by a federal agency, you may already have the necessary security and notification systems in place. If you are not federally regulated, you should assess the needs and requirements of your business. Primarily, you must understand the type of information your agency holds: do you have personally identifiable information or do you also maintain personal health information and/or payment card industry data? With whom do you have contracts and what security and notification procedures do those contracts require? How do you maintain this information? What laws must you comply with?

In Rhode Island, if you are covered by the Rhode Island Identity Theft Protection Act of 2015, you still have until July 2016 to institute a compliant system. Taking stock of and understanding the information your organization maintains and how it is maintained should be the first steps to implementing the appropriate system for your agency.

Date Created
April 5, 2016