



Chris Zoladz

Founder
Navigate LLC

The Challenge of Managing Our Service Providers and Our Service Providers' Service Providers

Nymity: What has changed in laws and regulations that make companies more directly accountable to ensuring that service providers and vendors are doing what they are saying when it comes to protecting personal information?

Zoladz: The most significant change that has occurred is the Massachusetts "Standards for the Protection of Personal Information of Resident of the Commonwealth" regulation that went into effect March 1, 2010. Specifically, the regulation requires that every company that owns, licenses, stores or maintains paper or electronic personal information^[1] concerning any Massachusetts resident "take reasonable steps to select and retain third-party service providers who are capable of, and agree in contract to, maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations." While it is believed many companies in highly regulated industries already have policies and procedures in place for assessing the security and privacy measures in place at their service providers that handle the personal information of their employees or customers, many companies in non-regulated industries do not. The most some companies have in place is broad security and privacy language in their agreements with the service providers and indemnification language, which is typically highly negotiated and rarely optimal. As a result, for companies in this state, they are non-compliant.

Nymity: Is this just a U.S. challenge or a global one?

Zoladz: I do not believe there is another law that is as specific as the Massachusetts regulation. However, I expect that in international markets that have federal privacy laws, such as the European Union, not considering the security and privacy measures in place at service providers would be a mistake. Setting aside any legal requirements, ensuring the protection of personal information within the company and at service providers is the right thing to do and ultimately in the best interest of the company.

Nymity: What must companies do to protect personal information? What are the key accountabilities?

Zoladz: Having a comprehensive and information security infrastructure in place is key. This includes meaningful policies, procedures, training, on-going communications, conducting risk assessments, remediating weaknesses and having a program of the on-going monitoring of the design and operating effectiveness of controls is required. The Privacy function needs to collaborate with the business unit managers and lead the effort in understanding the personal information lifecycle with third party service providers. The Security function then needs to help assess whether the service provider is meeting the expected security requirements. This may be accomplished by Security conducting a review at the service provider, reviewing a security self-assessment checklist completed by the service provider or reviewing a security review report produced by a third party.

[1] Defined in the regulation as "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."

Nymity: What must companies ask their service providers to do about their own processes and the processes for managing their service providers and so on to protect personal information?

Zoladz: From an information security perspective, service providers, and any service providers they use, which are sometimes overlooked, should be viewed as an extension of the company. This means they should be required to provide the same level of security that the company exercises over personal information within the confines of the organization. This includes having meaningful policies, procedures, training, on-going communications, conducting risk assessments, remediating weaknesses and having a program of the on-going monitoring of the design and operating effectiveness of controls.

Nymity: How many different kinds of service providers are we talking about? What types of service providers are they?

Zoladz: There are many different types of service providers that handle personal information of employees, customers and/or other stakeholders. For example, these service providers include, payroll processors, benefits administrators, health care providers, ecommerce service providers, online job application and recruiting services, restaurant reservation providers, stock transfer agents and others. Small companies may have only a few service providers that handle the personal information of their customers or employees while large companies may have hundreds of these service providers. Whether there are a small or large number of service providers used, the nature of the due diligence the company should be exercising is generally the same.

Nymity: Where do companies start? What is better than doing nothing?

Zoladz: For many companies the task of understanding and assessing the security controls at their service providers can be daunting because of the lack of resources to perform this work and/or the large volume of service providers being used. However, doing nothing or deferring until a later date is not prudent. The first step is to create an inventory of all the service providers that are handling personal information, including the nature of the information and the quantity. Using that information a ranking should be assigned. Specifically, the more sensitive the personal information (e.g., medical records) and the higher the volume of information the service provider handles, the higher the priority. With this information a phased approach can be put in place to engage the highest ranking service providers first in a discussion of the controls they have in place and a target date to then do the same with the next highest ranking service providers until all service providers have been covered.

Nymity: How do they resource the full set of accountabilities?

Zoladz: This is a challenge for companies of all sizes. For large companies, there are often a large number of service providers, sometimes hundreds. As a result, the amount of time to manage a service provider program can be significant. At small companies, the number of service providers is less but so are the available resources to manage them. In either case, the necessary resources will need to be identified using existing security and privacy staff, whether they are dedicated staff or not, external resources, or perhaps a combination. If internal resources can be used but cannot be dedicated to this effort, the more staff that can be identified to participate in the service provider program the easier it is to distribute the effort, accomplish your objectives and not overwhelm those that are assigned, or at least reduce the risk of overloading staff.

Nymity: How do they sustain their service provider programs?

Zoladz: This is a challenge. The most critical success factor to sustaining a service provider program requires that there are adequate resources to revalidate the existing service providers on some periodic basis (e.g., annually) and to also conduct the due diligence for new service providers. Using a standard repeatable process to obtain and review the necessary security information from the service providers will help ensure efficiency and maximize the ability to sustain the program.

Nymity: Are there some best practices or ways to minimize the expenses of the service provider programs?

Zoladz: Require the service provider to document and defend their security practices. Specifically, avoid conducting on-site reviews and instead require the service providers to provide security information in the form of a completed questionnaire signed off by an executive such as the CIO or CSO, or require the service provider to provide a third party review report. This places the burden with the service provider, which is where it belongs. After all, if the service provider's business is handling personal information they should not be surprised that their customers will want to understand how that information is protected and should be prepared and willing to "tell their story."

Nymity: In closing, do you have additional recommendations for companies, audit firms, standards bodies, various government agencies and other entities to help address the challenge of protecting personal information in an economic and effective manner?

Zoladz: My recommendation and hope is that there is a balanced view of the theoretical, practical and legal issues that surround the protection of personal information. This is a vitally important issue but should not unduly stifle economic growth, innovation, medical research, national security, or other programs that benefit society.