Six Myths about Data Privacy and Security that Professional Employer Organizations Should Skip

Wednesday, October 22, 2014

Data breaches and compliance failures threaten company reputation and put individuals’ personal identities, finances, and medical information in jeopardy. In the Professional Employer Organization (PEO) industry, where companies providing PEO or other human resource outsourcing services typically work with personal information of their employees as well as that of their customers’ employees, persistent myths can inhibit appropriate action. This article debunks some of those myths and encourages companies to take action.

**Myth 1: We are too small to be a target**

The size of a company, whether determined by number of employees, locations, or some other metrics, is not always the best measure of data risk. A small, solo health practitioner easily can maintain sensitive personal information on thousands of individuals. A neighborhood restaurant can process credit card data for hundreds of customers a week. A thinly staffed PEO can support many small business customers, handling personal information for thousands of employees.

An article in the Los Angeles Times pointed out that some small businesses may be more likely targets than larger organizations, even if their breaches do not make national headlines. E. Scott Reckard and Tiffany Hsu, Small businesses at high risk for data breach, Los Angeles Times, July 4, 2014. These companies are seen as having significant amounts of personal data, but employ less sophisticated safeguards and have fewer resources to react to an attack. The article noted, “But for every high-profile case, there are dozens of threats to confidential data held by everyday enterprises.”

**Myth 2: Other states’ laws do not apply to us**

When it comes to certain data privacy and security requirements, businesses cannot look only to federal law and the state laws in which they are located. PEOs often have employees or customers with employees (or dependents) who reside in other states, even if the PEO does not have locations in those states. Some states have enacted data protection laws that apply extraterritorially.

For example, the extensive privacy and security requirements of the Massachusetts data security regulations (201 CMR 17.00) apply to companies that “own or license” personal information about Massachusetts residents. According to the regulations, “own or license” refers to circumstances where a company receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment. Thus, a business that maintains personal information on a Massachusetts resident arguably must comply with those data security regulations, even if the business does not have a location or do business in the Bay state.

Therefore, PEOs and other businesses must review closely the kind of personal information they maintain, as well as the states of residency of the individuals to whom the information relates, to have a more complete understanding of their obligations.

**Myth 3: Our customers own the data; they have the reporting obligations**
All 47 state data breach notification laws provide that the obligation to notify affected individuals rests with the entities that own the personal information. Virtually every one of those laws also contains a notice requirement applying to entities that maintain personal information on behalf of the entities that own it. Thus, entities that maintain personal information and discover a breach of that information must notify the owners.

Determining which entity owns the personal information may not always be easy. If a PEO experiences a data breach pertaining to the personal information of its customers’ employees, it nevertheless must notify the affected customers or individuals under the applicable data breach notification laws. Additionally, PEOs may have contracted to take certain steps in the event of a data breach. Businesses are becoming increasingly aware of vendor risks and, regardless of the applicable statutes and which entity may be viewed as the owner of the data, they may determine by contract who is responsible for providing notification and taking other remediation steps to resolve the breach.

This is a critical issue for PEOs because a breach can involve personal information of employees working at one or more of their customers. Getting notices out in this context needs coordination between the PEO and its customers. Determining what happened, who will provide the notice, whether to provide credit monitoring, and so on, all can cause significant delays in the notification process. As with other risks and exposures that exist and may be shared between PEOs and their customers, PEOs may want to be proactive and develop a mutually agreeable approach to breach response. This would go a long way toward limiting delays and avoiding potential government agency inquiry and private lawsuits related to delayed notifications.

**Myth 4: It’s enough that our handbook’s privacy policy requires strong passwords**

Having a well-drafted handbook policy and a requirement for strong passwords is a good start, but that is insufficient to satisfy just about any of the data security standards required under federal or state law. In states such as California, Connecticut, Florida, Maryland, Massachusetts, and Oregon, a written information security program (WISP) in one form or another is required.

WISPs start not with policies, but assessments. That is, even before an organization puts pen to paper or finger to keyboard to create a policy or policies, it must assess the risk the personal information it maintains poses. Along with other considerations, this includes learning more about the kinds of personal information the company maintains, who has access to it, and how and where is it being stored. At that point, the company can better address the administrative, physical, technical, and organizational risks to that information in the form of policy — a WISP.

For many PEOs, a WISP can be a competitive advantage, benefiting existing and potential customers. A company with a WISP often can better defend against claims related to a data breach, help the company manage and safeguard critical information, and may even avoid employee whistleblower claims.

**Myth 5: Our IT Department is on top of this**

An organization’s information technology (IT) department is critical to safeguarding all of the organization’s information assets. However, leaving that responsibility solely in the hands of the IT department presents certain problems, including:

- The increasing complexity of IT systems often makes it difficult for upper management to understand an organization’s needs and whether its IT department is addressing those needs or has the expertise to do so.
- Putting data privacy and security in the silo of an IT department may stifle collaboration among other departments, making it difficult to identify risks as well as solutions.
- IT departments may not be able to keep up to date with and apply legal developments.
- Fearing discipline, IT departments may hesitate to address data incidents or may be too aggressive in downplaying risk of harm.

Data privacy and security is an enterprise-wide issue requiring the involvement of key stakeholders in the organization. Further, even if the PEO’s IT department is top-notch, the PEO cannot monitor what is going on at its customers’ facilities and be prepared if a breach affects its customers.

**Myth 6: Our insurance covers these situations**

Like many other risks, information risk can be addressed in part through insurance. Increasingly, carriers are offering products designed to deal with personal information risk and, specifically, data breach response.
However, do not assume your current policies cover data breaches. A company claiming data breach coverage under its commercial general liability policy found in a New York courtroom that it did not. However, another company making similar claims under a similar policy was found by a federal district court in California to be covered under the policy.

Thus, companies should understand the coverage they have and the coverage they select and work closely with their brokers and appropriate counsel. Coverage known as “cyber” coverage may cover costs incurred in responding to a data breach (e.g., notification, legal, media, and credit monitoring). Even if the policy addresses such costs, it may not cover exposure to litigation and regulatory investigations. PEOs considering such insurance should confirm application of the coverage to the personal information they maintain, as well as that which they may maintain on behalf of customers. PEOs also should make sure the coverage is in line with obligations in customer service agreements.