Fact or Fiction:

Uncovering the Myths about Data Privacy & Security that PEOs and Your Co-Employers Should Avoid

Data breaches and compliance failures continue to threaten companies and put individuals' personal identities, finances, and medical information in jeopardy. For companies that experience those breaches, reputational harm can have a significant impact on their business. This is true in most industries, including the Professional Employer Organization (PEO) industry, where companies that provide PEO or other human resource outsourcing services typically are swimming in personal information belonging to their employees, as well as that of their customers' employees. However, perceptions about risk can inhibit appropriate action. Some of those perceptions derive from common myths about data security that all companies, including PEOs and their Co-employers, should avoid.

Myth #1: A PEOs' Co-employers are too small to be a target.

The size of a company, whether measured by number of employees, locations or certain 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 per week. A thinly-staffed PEO can support many small business customers, involving the handling of personal information for thousands of employees.

This point was made clear in a recent L.A. Times article, and should not be overlooked. Certain small businesses may be more likely to become targets than larger organizations, even if their breaches do not make national headlines. These companies are viewed as having significant amounts of personal data, with less sophisticated safeguards in place and fewer resources to handle an attack.

> ***"But for every high-profile case, there are dozens of threats to confidential data held by everyday enterprises."***
>
> ***--L.A. Times***

Myth #2: Our Co-employers own the data, and they have the reporting obligations.

It is true that all of the 47 state data breach notification laws provide that the obligation to notify affected individuals rests with the entities that own the personal information. However, virtually all of those laws also contain a notice requirement applying to entities that maintain personal information on behalf of the data's owners. In that case, entities that maintain personal information and discover a breach of that information must notify the owner(s).

The determination of which entity owns the personal information may not always be an easy one. But, either way, if a PEO or their Co-employer experiences a data breach pertaining to the personal information of its customers' employees, it will have to notify the customer(s) under the applicable data breach notification laws. Additionally, PEOs

and their Co-employers may have contract obligations that require them to take certain steps in the event of a data breach. Businesses are becoming increasingly aware of vendor risks. As a result, regardless of the applicable statutes and what entity may be viewed as the owner of the data, these businesses seek to determine by contract what entity is responsible to provide notification and take other remediation steps to resolve the breach.

Entities that maintain personal information and discover a breach of that information must notify the owner(s).

This is a critical issue for PEOs and their Co-employers because a breach can involve personal information of employees working at one or more of their customers' companies. In this context getting notices out can be challenging due to coordination needed between the PEO and its customers. Determining what happened, who will provide the notice, whether to provide credit monitoring, and so on, 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 take a more proactive approach and develop a mutually agreeable tactic to breach response. This would go a long way toward limiting delays and avoiding potential agency inquiry and private lawsuits related to delayed notifications.

Myth #3: Our IT Department is on top of this.

No doubt, an organization's IT Department is critical to the process of safeguarding all of the organization's information assets. However, leaving that responsibility solely in the hands of IT personnel can be problematic for a variety of reasons:

- The increasing complexity of IT systems often makes it very difficult for senior 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 in a position to keep up to date with legal developments or know the best method to apply them.

Fearing discipline, IT departments may not be as quick to address data incidents or may be too aggressive in downplaying risk of harm.

Data privacy and security is an enterprise-wide issue that requires the involvement of key stakeholders in the organization. Furthermore, even if the PEO's IT department is top-notch, the PEO cannot monitor what is going on at the customer's facilities. All they can do is be prepared to be brought into a breach should one occur.

Myth #4: We have a privacy policy in our handbook and require strong passwords, so we are good.

Having a well-drafted handbook policy and a requirement for strong passwords is a good start. But, those two items by themselves are insufficient to satisfy most 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 do not start with policies, but with assessments. That is, even before an organization puts pen to paper or finger to key to create a policy or policies, it must assess a number of factors concerning the risk the personal information it maintains poses.

This includes learning more about the kinds of personal information the company retains, who has access to it, how and where it is being stored, along with a number of other considerations. At that point, the company is in a better position to address the administrative, physical, technical and organizational risks to that information in the form of policy…a WISP.

For many PEOs and their Co-employers, a WISP can be a competitive advantage by providing comfort to existing and potential customers concerning the safeguarding of personal information. A WISP also will better position a company when defending claims related to a data breach, help the company manage and safeguard critical information, and may even help avoid whistleblower claims from employees.

A WISP can be a competitive advantage by providing comfort to existing and potential customers concerning the safeguarding of personal information.

Myth #5: Our insurance and our Co-employers' insurance covers these situations.

Like many other risks, information risk can be addressed in part through insurance. Increasingly, carriers are developing products designed to deal with personal information risk, and specifically data breach response. Acquiring this kind of coverage certainly should be considered by any organization as part of its plan to address information risk.

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 must be careful about understanding the coverage they have and the coverage they select; they should be working closely with their brokers and appropriate counsel. Coverage known as "cyber" coverage is not necessarily going to cover costs incurred by the company to respond to a data breach.

Do not assume your current policies cover data breaches.

And, even if the policy addresses costs the company incurs to respond to a breach (notification, legal, media, credit monitoring, etc.), it may not cover exposure from litigation and regulatory investigations. For PEOs and their Co-employers considering such insurance, it will be important to confirm application of the coverage to their personal information, as well as that which they maintain on behalf of customers. PEOs and their Co-employers also will want to be sure that the coverage is in line with their customer service agreements.

Myth #6: We are located in State X, and laws in other states do not apply to us or our Co-employers.

When it comes to certain data privacy and security requirements, businesses cannot look solely to federal law and the state laws in which they are located. PEOs often have employees or have customers that have employees (or dependents of those employees) who reside in a number of states, even if the PEO does not have locations in those states. However, some

states' data protection laws are being applied extraterritorially.

For example, the Massachusetts data security regulations (201 CMR 17.00) set forth extensive privacy and security requirements that apply to companies that "own or license" personal information about Massachusetts residents. According to the regulations, the term "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 concerning a Massachusetts resident arguably must comply with those data security regulations, even if the business does not have a location in the Bay state or does not do business there.

For this reason, PEOs and other businesses need to look closely at the kind of personal information they maintain, as well as the state(s) of residency of the individuals to whom the information relates, in order to have a more complete understanding of its obligations.

Summary

What PEOs and Co-employers may think of as fact is really fiction, for there are multiple myths with regard to data breach risks and responsibilities. The personal data that PEOs and Co-employers maintain requires them to take certain precautions.

It is important to realize that small firms are being targeted as much, if not more, than large ones. It is critical to examine the states of residence of those in the firms' databases. PEOs and their Co-employers are responsible for notification just as much as the customers themselves.

A Written Information Security Program (WISP) should be incorporated into company policies. Organizations should not rely solely on their IT department for breaches. They should examine their insurance policy and acquire the appropriate protection, if needed.

By debunking these myths, PEOs and Co-employers can see the truth and take the proper action.

About the Author

Joe Lazzarotti is a partner with the Jackson Lewis law firm and head of its Privacy, eCommunications and Data Security Practice Group.