Key Data Privacy and Security Issues for PEOs

Joseph J. Lazzarotti, Esq.

Information risks relating to such things as data breaches, compliance failures, and reputational harm continue to threaten companies and put individuals' personal identities, finances, and medical information in jeopardy. Addressing this issue immediately and in the coming years is a significant and worthy endeavor for any business. This is particularly true in the PEO industry, where companies that provide PEO or other human resource outsourcing services typically are swimming in the personal information of their employees, as well as that of their client's employees. The following list, which is by no means exhaustive, provides 10 critical areas businesses need to consider when addressing this issue.

Risk Assessment

Many businesses remain unaware of how much personal and confidential information they maintain, who has access to it, how it is used and disclosed, how it is safeguarded, and so on. For PEOs, being responsible for many clients and the personal information of thousands of employees is not uncommon, but finding the answers to questions concerning that personal information can be daunting. Getting a handle on a business' critical information assets must be the first step, and it is perhaps the most important step to tackling information risk. You simply can't adequately safeguard something you are not aware exists.

Develop a Written Information Security Program

Even if adopting a written information security program (WISP) to protect personal information is not an express statutory or regulatory mandate in your state, having one is critical to addressing information risk. For many PEOs, a WISP can be a competitive advantage by providing comfort to existing and potential clients concerning the safeguarding of their employee's 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 avoid whistleblower claims from employees. In states such as Massachusetts, Oregon, and Connecticut, a WISP in one form or another is required. If your PEO clients have employees residing in one of these states or others that require WISPs, you should have a WISP that is compliant with the applicable state law.[1]

Vendors/Business Partners

Businesses addressing their information risk cannot stop at the proverbial "doorstep"—their information systems, buildings, and employees. Very often, vendors maintain significant amounts of sensitive company and personal information for their clients. This list of vendors can be long and include vendors such as: employee benefits consultants, administrators, and brokers; accountants; lawyers; record storage/destructions companies; office cleaning services; payroll companies; and cloud computing or other information service providers.

PEOs use many of these same vendors, and in some instances may be vendors themselves. Any business that turns over sensitive information to a vendor needs to take steps to ensure the vendor has implemented appropriate safeguards to protect the information. Likewise, vendors receiving such information need to take appropriate steps. If the information is personal information, a number of states mandate contract provisions requiring the vendor to safeguard the information. PEOs, therefore, need to look out for these provisions in their service contracts, as well as in contracts with their own vendors.

The Health Insurance Portability and Accountability Act (HIPAA)

The recent changes under the American Recovery and Reinvestment Act (ARRA) of 2009 will drive increased focus onto HIPAA in 2010, particularly for business associates that for the first time become directly subject to many of the same privacy and security requirements as covered entities. The addition of a HIPAA breach notification requirement, effective September 23, 2009, already is driving covered entities to amend their business associate agreements, and business associates to adapt to the new procedures. For PEOs, many of which manage healthcare coverage for their clients, this will be a significant challenge.

Insurance

Like many other risks, information risk can be addressed in part through insurance. More carriers are developing products dealing with personal information risk, and specifically data breach response. This kind of coverage should be a part of any information officer's, privacy officer's, or risk manager's plan for safeguarding information.

Identify 'Red Flags'

Identifying "red flags" is the next step after implementing a WISP, beyond safeguarding sensitive information. The concept of "red flags" is having policies and

1 See also *NAPEO Legal Review,™* "Workplace Data Protection and Responsibilities," available to members at *www.napeo.org/members/secureDocument.cfm?docID=740.*

procedures designed to detect, prevent, and mitigate instances of identity theft—that is, with safeguards already in place, businesses need to be able to identify circumstances ("red flags") that indicate incidents of identity theft could be occurring, and then take steps to prevent the identity theft or mitigate its effects. After a number of extensions, on June 1, 2010, the Federal Trade Commission will begin enforcing its "red flag" regulations that apply to financial institutions and creditors. PEOs need to carefully review whether they are "creditors" that maintain "covered accounts.[2]"

Training

A necessary component of any WISP and a required element under most federal and state laws mandating data security is training. Training deserves special mention if only to remind employees how powerful the small devices are that they carry around.

Develop a Plan for Responding to a Breach Notification

All state and federal data breach notification requirements currently in effect require notice be provided as soon as possible, as well as a number of other steps. Delays in notification that are viewed as unreasonable could trigger an inquiry by the state's attorney general, or in the case of HIPAA protected health information, the office of civil rights.

This is a critical issue for PEOs because in most cases, a breach involves the personal information of employees working at one or more of their clients. Getting notices out in this context can be challenging because of the coordination needed between the PEO and its clients. Determining what happened, who "owns" the information, who will provide the notice, paying for the monitoring, and so on, all can cause significant delays in the notification process. A clear procedure the PEO communicates to its clients would go a long way toward limiting delays and avoiding potential agency inquiry and private lawsuits related to delayed notifications.

Carefully Integrate New Technologies

As businesses look for new technologies to increase productivity, cut costs, and gain a competitive advantage, how those technologies address information risk must be a factor in the decision whether to adopt the technology. For example, cloud computing is fast becoming a popular tool used by businesses to enhance their computing capabilities, in some cases at substantially reduced costs, but it raises a number of issues concerning information risk.

Watch for New Legislation

Today, managing data and ensuring its privacy, security, and integrity is critical for businesses and individuals, and is increasingly becoming the subject of broad, complex regulation. It seems to be only a matter of time before U.S. companies are subject to a national law requiring the protection of personal information. Companies therefore need to stay tuned to remain compliant and competitive in this regard.

For example, under a measure passed overwhelmingly by the U.S. House of Representatives (408-13), the Secure Federal File Sharing Act (H.R. 4098), PEOs that are federal contractors would be required to adopt measures established by the Office of Management and Budget to limit open network peer-to-peer file sharing software (P2P Software). Congress also is considering legislation, the Data Accountability and Trust Act (DATA) (H.R. 2221), that would preempt all state notification laws and instead establish a national breach notice standard. DATA also would impose heightened requirements for safeguarding personal information, such as:

- A policy concerning the collection, use, sale, other dissemination, and maintenance of such personal information;
- Naming an officer or other point person to manage information security;
- Developing a process for identifying and assessing any reasonably foreseeable vulnerabilities in the person's electronic systems, include regularly monitoring for breaches of security;
- Having a process for taking preventive and corrective action to mitigate against any such vulnerabilities; and
- Implementing a process for disposing of obsolete electronic data containing personal information.

Federal and state regulation of the use, disclosure, and safeguarding of the privacy and security of personal information will no doubt continue to grow. Businesses, particularly those with a presence in more than one state and or country, such as PEOs, will need to evaluate the kinds of information they maintain both for their businesses and their employees, and track the applicable legal developments. Appropriate policies and procedures, among other steps, such as developing a breach response plan, can go far in reducing potential liability.●

Joseph J. Lazzarotti, Esq. is a partner in the White Plains, New York, office of Jackson Lewis, LLP.

2 See also *NAPEO Legal Insights,™* "'Red Flags Rule' Overview," available to members at *www.napeo.org/members/secureDocument.cfm?docID=1032*, for potential requirements under the Fair and Accurate Credit Transactions Act of 2003 (FACTA).