MILLER COOPER & Co., Ltd
ACCOUNTANTS AND CONSULTANTS

NEWS & VIEWS

Commitment Focus Continuity Passion

Miller Cooper Nonprofit News

May 2017

By Susan R. Jones, CPA, Principal

Data Security Risk Assessment and Management

Getting a handle on technologies that are transforming organizations is critical to understanding how your entity should manage privacy. New devices containing personal information that are used both at home and at work are blurring the line between the two. The same is true of devices that are networked, or “smart” and interactive. Their use may result in the unintended transfer of personal information to employers, service providers, vendors or others.

Personal information may also be held in a host of repositories on the web, and many of those sites provide new ways to connect and interact with such information. The result: more personal information in more places under the control of more entities. For example, while cloud computing affords new economies and efficiencies to information processing, it also spreads the custody and control over personal information well beyond the organization’s traditional boundaries. These technologies are not only changing organizations, they are changing who and what has custody and control over personal information. Therefore, they are also changing the way that organizations manage privacy.

The loss, theft or breach of personal information can damage an organization’s reputation. Lost productivity, lost revenue and media scrutiny are a few of the consequences when there is a data breach or loss of personal information. In addition, mounting regulations requiring policies and

procedures that ensure the security of personal information should make privacy concerns a top priority.

While there is no way to absolutely prevent a data breach, the organization can mitigate its risk of a data breach by understanding data security, privacy and the protection of personal information. As an example, knowing how identity theft takes place, the impact it can have on your organization and how the stolen information is used is critical in preventing identity theft. With that in mind, the following list (which is by no means exhaustive) provides critical areas management and boards should consider when developing a privacy risk management plan.

Establishing a Technology and Risk Assessment Policy

- ***Risk Assessment.*** Many organizations 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. Getting a handle on your organization's critical information assets must be the first—and is perhaps the most important—step when tackling privacy risk.
- ***A Written Privacy Risk Management Program.*** Even if adopting a written privacy risk management program to protect personal information is not an express statutory or regulatory mandate in your state, having one is critical to addressing privacy risk. Not only will such a program better position the organization when defending claims related to a data breach, but it will help your entity manage and safeguard critical information. In addition, such a program can be publicized to demonstrate commitment to constituency privacy.

- ***Training.*** Training is a necessary component of any privacy risk management plan and a required element under most federal and state laws that address data security. Employees should be trained to understand the risks to private information they carry around in mobile phones, electronic tablets, laptops and other electronic devices used for organizational purposes and how to safeguard such information.

Implementing Technology and Risk Assessment Policy

- ***Vendors.*** Your organization may be especially vigilant about screening employees and performing background checks. Be certain that background screening is being conducted by the

companies you contract with as their employees will have access to your physical—and sometimes electronic—locations where personal information may be accessed. If your organization entrusts sensitive information to such vendors, management needs to take steps to ensure the vendor has implemented appropriate safeguards to protect the information.

- ***Insurance.*** Like many other risks, information risk can be addressed in part through insurance. More carriers are developing products dealing with privacy risk management and, specifically, data breach response. This kind of coverage should be a part of management and the board's considerations when establishing a privacy risk management plan.
- ***Policies and Procedures to Warn of Potential Breaches.*** The organization should have policies and procedures designed to detect, prevent and mitigate instances of identity theft. In other words, the organization should have a process in place to identify circumstances that indicate incidents of identity theft could be occurring and then take steps to prevent it or mitigate its effects.
- ***Carefully Integrating New Technologies.*** As organizations look for new technologies to increase productivity, cut costs, and better serve their constituency, how those technologies address privacy risk and data breaches should be a factor in the decision whether to adopt the technology.

Responding to a Security Breach

- ***Plan for Responding to a Breach Notification.*** Even the best-run organizations may suffer from a breach of private information. Thus, the need for effective and timely management of such breaches. All state and federal data breach notification requirements currently in effect require notice be provided as soon as possible. Delays in notification 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. Management, with the approval of the board, should develop a formal, effective and repeatable plan to determine the nature of a breach and the steps to take in response to it. In addition, management should ensure that staff is well trained so that they know what might constitute a breach that warrants the attention of management. The absence of such a plan may open the organization up to further damage than is warranted by a situation.

Technology and Data Security Requires Vigilance Managing data and ensuring its privacy, security and integrity is critical for organizations and is increasingly becoming the subject of broad, complex regulation. It seems to be only a matter of time before all U.S. entities are subject to a national law requiring the protection of personal information. Therefore, management and the board should continue to monitor the status of new and proposed legislation to remain compliant.

For more information, please contact Susan Jones at SJones@MillerCooper.com or 847-205-5000.