Ensuring Privacy in an IT World

AICPA Insights - Posted by Jocelyn Woodard on Sep 04, 2013

Do you expect a right to privacy? Do your clients? The truth of the matter is that the right to privacy is an ever-changing, ever expanding concept that continually needs to be redefined. That's especially true when it comes to ensuring privacy in an IT world. Ensuring privacy, which concerns the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information, comes with risks.

Managing Privacy Risks

A breach of privacy from mobile technology data leaks, data breaches in the organization, a cyber-attack or other causes could result in the unauthorized disclosure of personal information about employees, clients and others. Managing that risk is important for everyone. In fact, the issue of ensuring privacy was ranked fourth in the U.S. and sixth in Canada according to the AICPA 2013 North America Top Technologies Initiatives Survey.

According to the survey results, 82% of the respondents, most of whom identified themselves as an Executive/Partner, Director/VP or Manager in public accounting or business and industry, said that they "frequently or regularly" encountered information technology questions or concerns in their field of work. Only 16% reported that their encounters were "minimal" and an even smaller percentage (2%) responded that the issue has "never" been a concern.

Establishing Privacy Policies

To protect privacy, organizations should establish privacy policies that address privacy laws and requirements, put privacy safeguards and controls in place and secure data and systems. For example, public accounting and business and industry firms can protect themselves and their clients' information by developing and implementing policies addressing client information, automated monitoring of access and use of information and employee awareness training.

They can also perform privacy audits based on Generally Accepted Privacy Principles to help clients assess their risks. Most importantly, if there is a privacy breach, an organization must be prepared to respond to the threat within their IT environment. But, how do organizations that do respond – do it effectively?

Responding Versus Preventing

Responding to a privacy breach will depend upon the nature of your organization, the types of data you use and the number of employees you have to respond. While responding to a privacy breach is important, *preventing* it from happening in the first place is generally a better goal. According to the *Journal of Accountancy,* the following steps can help organizations in both public accounting and business and industry ensure privacy and mitigate the risk of a potential reputation-damaging data breach:

1. Identify and classify the types of information the firm maintains
2. Assess your current controls and the threats facing high-risk data
3. Upgrade protection strategies as needed
4. Review the impact of vendors and third-party service providers
5. Know the requirements of applicable data privacy protection laws and regulations
6. Destroy sensitive or confidential data when it is no longer needed
7. Develop, implement and test an incident-response plan

To assist CPAs in this effort, the AICPA has developed an Incident Response Plan Template which outlines how to create an incident response plan, how to assemble a team to address the issues and define their responsibilities, how to go about notifying those affected and other issues that may pertain to your situation.

Need more information on privacy issues? The AICPA / Canadian Institute of Chartered Accountants Privacy Task Force has created numerous tools, ranging from high-level questionnaires to Generally Accepted Privacy Principles, to help you and your clients manage privacy risks. The AICPA has also developed a Privacy Principles Scoreboard, which will help organizations and the CPAs that serve them attain best practices in the assessment and management of privacy.

Jocelyn M. Woodard, Manager IMTA, American Institute of CPAs. *Jocelyn is a technology risk and assurance manager assisting AICPA committee and task force members with the planning and implementation of initiatives that will better aid CPAs in understanding and utilizing information management and technology assurance tools and concepts.*