Journal of Accountancy

# Protecting privacy

BY JOEL LANZ, CPA/CITP AND NANCY A. COHEN, CPA/CITP

August 1, 2012

Under pressure from regulatory requirements, professional standards, and client expectations—not to mention increasingly sophisticated hackers—CPA firms are emphasizing efforts to protect the privacy of confidential information under their purview. The following steps can help firms mitigate the risk of a reputation-damaging data breach:

✔ **Identify and classify the types of information the firm maintains.** Firms should understand the information they keep and define what types of information should be protected. In most cases, firms can use a scheme of three to four categories (e.g., restricted/sensitive, confidential, internal use, and public) to classify information and prioritize protection efforts. Challenges include identifying other locations, such as audit work papers, that can contain nonpublic information.

✔ **Assess your current controls and the threats facing high-risk data.** Consider threats from external and internal perspectives. Many firms, based on media accounts, recognize threats caused by potential hacker and malware efforts. However, employees can inadvertently "leak data" by misplacing files, using personal storage media (such as smartphones and flash drives), or transferring data outside the firm.

✔ **Upgrade protection strategies as needed.** To protect themselves and their clients' information, more firms are developing and implementing policies addressing client information, automated monitoring of access and use of information, and employee-awareness training. Technical solutions such as monitoring and data-leakage protection software may also be considered. In light of the sophistication of evolving threats, cyber insurance frequently is sought.

✔ **Review the impact of vendors and third-party service providers.** With the advent of cloud computing, many firms now rely on third parties to host, manage, and protect their data. Although functions can be contractually assigned to a third party, accountability for data protection cannot. Firms should address the issue of accountability by ensuring that their contracts with third-party providers include data protection expectations such as service-level agreements that hold the service provider to the same standards of information protection as the firm.

✔ **Know the requirements of applicable data privacy protection laws and regulations.** Firms need to be aware of the implication of regulations such as the Gramm-Leach-Bliley Act (see aicpa.org/privacy (http://www.aicpa.org/privacy)) and should also be cognizant of the data breach laws in the states where their clients reside. Many state data breach notification laws are applicable based on where the individual resides rather than on where the firm does business or where the breach occurred.

✔ **Destroy sensitive or confidential data when it is no longer needed.** At the end of the retention period,

the information should be returned to the client or properly destroyed. Paper documents should be shredded with a cross-cut shredder. Before disposing of devices, remove all electronic data using methods such as secure data-wiping software.

✔ **Develop, implement, and test an incident-response plan.** Privacy breaches can occur despite the best prevention efforts. Creation of an incident-response plan enables firms to develop optimum strategies to respond on several fronts, including regulatory and public relations.

*(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 firms and their clients manage privacy risks. Access these tools at aicpa.org/privacy (http://www.aicpa.org/privacy).)*

*—By **Joel Lanz**, CPA/CITP, ( jlanz@joellanzcpa.com (mailto:jlanz@joellanzcpa.com) ) an adjunct professor at the State University of New York–College at Old Westbury and chair of the AICPA CITP Credential Committee, and **Nancy A. Cohen**, CPA/CITP, ( ncohen@aicpa.org (mailto:ncohen@aicpa.org) ) an AICPA manager.*