

# The Practicing

# CPA

THE NEWSLETTER OF THE AICPA PRIVATE COMPANIES PRACTICE SECTION



pcps.aicpa.org

February/March 2010

## Inside

- 3 The FBI and the ABA advise companies to designate a sole computer for online transactions.
- 3 A link to an AICPA article that helps clients to understand their tax issues.
- 4 CPA firms can use a blog to maintain relationships with current clients and to attract new business.
- 5 Managers who “friend” with employees on social networks need to avoid relationships that could create legal problems.
- 5 A reminder to practitioners that in December 2009, the AICPA released the 2009 edition of the *Compilation and Review Developments* alert.
- 6 The Ohio Society of CPAs launches initiatives to help CPAs promote their services. Also, a new tax benefit for military personnel.
- 8 CFOs will expand outsourcing in 2010.
- 8 Register Now for Practitioners Symposium.

### PCPS Update

- 7 Don't Miss These Great Resources for PCPS Members ♦

## Adding Privacy Leadership Services to Your Firm's Practices

*Lyndon Group has faced the current recession by adding a new service to help businesses halt customer identity theft.*

**B**ased in Newport, CA, Lyndon Group ([www.Lyndon-Group.com](http://www.Lyndon-Group.com)) is an accounting, finance, IT, and corporate governance professional services firm specializing in project-based engagements. Lyndon Group serves both public and private companies and has professionals engaged at some of the best known companies in the world, as well as middle market and emerging growth organizations. The firm has been very successful over the last nine months at launching several new service areas and divisions tailored to different sizes of businesses (predominantly smaller businesses).

Lyndon Group's practice areas span a wide range of sophisticated business areas, including accounting, finance, IT, governance, risk, and compliance. On August 11, 2009, the firm announced the addition of a practice area specifically tailored for the region's small and middle-market businesses: privacy leadership services.

The new service offering empowers businesses to reduce the risk of customer identity theft and data misuse and mismanagement. Larger businesses generally have the wherewithal to acquire technology and employ full time manpower to execute security and privacy policies effectively. However, small and midsize businesses more likely need assistance and direction from the outside.

Recently, IndyStar.com reported that “A rising swarm of cyber-robberies targeting small firms, local governments, schools, faith groups,

and nonprofits has prompted an extraordinary warning. The American Bankers Association and the FBI are advising small and midsize businesses that conduct financial transactions over the Internet to dedicate a PC to use only for online banking.” (See “Designate a Computer for Online Transactions” on page 3.)

### Privacy's Effect on the Bottom Line

Lyndon Group's new practice area focuses on helping small and midsize businesses understand why privacy is important to a company's bottom line. Client companies also gain an understanding of industry-specific privacy issues and the steps to take to develop an ongoing privacy and risk mitigation program addressing current and future requirements.

Every company that collects, manages, shares, or stores personal information faces significant risk from failing to comply with regulatory and legal requirements. The risks include damage to a company's reputation and brand and business relationships, legal liability and industry or regulatory sanctions, charges of deceptive business practices, and customer or employee distrust.

Many prospective clients are unaware of the monetary and image damages associated with a data breach. A damaged brand or reputation, according to the findings of the Ponemon Institute's *National Survey on Data Security Breach Notification*, can have a negative effect on clients and customers who are notified of a data breach.

*continued on next page*

*continued from page 1*

The Ponemon survey found that such notification causes almost 20% of clients and customers to plan to or actually end their relationship with the breached company.

In addition, a firm victimized by data theft may face the costs of legal fees and possible restitution, as well as management and employee distraction. The costs to some victimized small companies have reached \$1 million, according to Eric Nelson, practice leader of Lyndon Group's Privacy and Information Security practice.

"The Identity Theft Resource Center reported a 47% increase in data breaches in 2008 [compared with] 2007, but the surprising fact is that the majority of these breaches are not attributable to hackers, but to mismanagement and misuse of personal information relating to people, processes and policies," Nelson said. "Individuals expect their privacy to be respected and their personal information to be protected. With almost daily reports of identity theft, they are no longer willing to overlook a company's failure to protect their privacy and personal information."

Employees also might feel the negative effect of a company's failure to protect privacy and personal information. In a time of recession, maintaining employee morale is very important. When employees see their employer's concern for securing personal information, they will think of the company as having respect for clients and employees. Such satisfied employees are not only likely to do their jobs well and be productive but also are less likely to be absent or seek employment elsewhere.

Perhaps more important, satisfied employees and an effective privacy and security program also can help to prevent damage. Unhappy employees, including ex-employees, sometimes express their discontent by being destructive.

### Staying Attractive

At all times and perhaps more importantly in a time of recession, a company wants to present a picture of "good health" to prospective acquirers. Would-be acquirers might turn away if a prospective acquisition has weak security controls and penetrable privacy policies, a damaged reputation, or discontented employees.

### The Privacy Program

Elements of Lyndon Group's privacy leadership program include the following:

- Development of an inventory of privacy-related assets
- Assessment of existing system controls to identify and document internal and third party information safety risks
- Classification of the company's privacy related information
- Recommendations for preventing and responding to data breach incidents
- Finalization of ongoing privacy best practices to align with the business's culture and maintain customer trust
- Identification of state, federal, and international privacy requirements

### Privacy Resources

The following resources offer guidance on helping clients protect privacy:

- Eric Nelson, CIPP, "Protecting a Business and Maintaining Clients' Trust," *The Practicing CPA*, November 2009
- AICPA Information Technology Center (see <https://infotech.aicpa.org/Resources/Privacy/Federal+State+and+Other+Professional+Regulations/Fair+and+Accurate+Credit+Transactions+Act+of+2003/Identity+Theft+Red+Flags.htm>)
- Records management (see the paper on using generally accepted privacy principles in records management which can be downloaded from the AICPA IT site at <https://infotech.aicpa.org/Resources/Privacy/Privacy+Services/Records+Management.htm>)
- Individual states. Link to information safeguard and breach notification requirements from the AICPA: click on **State Security Breach Laws**

The guidance offered on the AICPA Information Technology Center Web site is oriented to CPAs who may be involved with helping clients decide whether they need to and how to comply with regulations.

*Editor's note: Eric Nelson, CIPP, and Kenneth L. Jones, CPA, founder and executive managing director of Lyndon Group, contributed to the preceding article.*

*The Practicing CPA* (ISSN 0885-6931) February/March 2010, Volume 34, Number 2. Publication and editorial office: 220 Leigh Farm Road, Durham, NC 27707. Copyright © 2010 AICPA. Opinions of the authors are their own and do not necessarily reflect policies of the AICPA.

**Editor:** William Moran.

**Editorial Advisors:** William R. Pirulli, Warwick, RI; Barry D. Beck, Woburn, MA; Peggy A. Dzierzawski, Troy, MI; Jina Etienne, Silver Spring, MD; Kevin R. Heppner, Madison, WI; Scott W. Kies, Tucson, AZ; Victoria A. Martin, Hickory, NC; Dennis K. Meservy, Las Vegas, NV; Marc Parkinson, San Jose, CA; Phillip J. Santarelli, Philadelphia, PA; Melody D. Schneider, Fairbanks, AK; Jerry A. Topp, Fargo, ND; George S. Willie, Washington, DC; Lee D. Wunschel, Toledo, OH; Michelle L. Zimmerman, Indianapolis, IN