JOURNAL OF ACCOUNTANCY

PROFESSIONAL LIABILITY SPOTLIGHT

A breach of client data: Risks to CPA firms

BY AMY WALDRON, CPA, AND DAVID HALLSTROM

AUGUST 2013

You walk into your office on a Saturday morning during tax season to find a staff member waiting for you with sweaty palms and a look of terror on her face. She takes a while to get the words out, but you soon learn that she backed up some client files to an unencrypted flash drive and dropped it in her purse before going to a "happy hour" the night before. Upon returning to her table from the restroom, she discovered her purse was nowhere to be found. She had been preparing payroll tax returns for several clients with multistate locations, and the flash drive contained payroll data such as names, Social Security numbers, addresses, salaries, and wages.

You have a lot of questions. What other data were on the flash drive? Which records were exposed? What information should be shared with your staff? How should they respond to related inquiries? How and when should the firm break the news to affected clients? Other questions may not immediately come to mind but are still very important. Is the clock ticking on state law requirements to notify affected businesses and individuals? Does state law require you to offer credit monitoring services to affected individuals?

COMMON DATA BREACH SCENARIOS

CPA firms have made great strides in embracing technology. Electronic data management systems, client portals, and cloud-computing systems foster an ease of doing business. However, records maintained by firms must remain confidential because of professional standards, statutes, and regulations governing record retention. Data breaches can happen in numerous ways, including the following: a lost or stolen device, hacking, fraud, improper disposal of data, and errant email messages. It may be only a matter of time until you face a similar breach.

A FIRM'S EXPOSURE

A CPA firm faces numerous exposures in the event of a data breach:

Claim for damages. A client or third party can bring both direct claims and cross-claims for indemnification against the firm for damages incurred as a result of the exposure.

Direct claims may relate to costs incurred to investigate and mitigate damages that could be attributed to the breach, including forensic services, public relations expenses, and costs incurred to place affected parties on notice of the breach and provide credit monitoring services. Damages also may be sought for lost business directly related to the breach, or indirectly related, such as those arising from a disclosure of trade secrets.

Cross-claims for indemnification may arise from individual or class action lawsuits filed against the client by employees or customers. These claims typically allege failure to secure confidential data, resulting in identity theft or loss of business. Clients also may encounter civil and criminal enforcement proceedings if regulators such as the Federal Deposit Insurance Corp. (FDIC), Federal Trade Commission (FTC), the Department of Health and Human Services (HHS), or SEC deem the client was responsible for the breach. Legal costs to defend such proceedings can be substantial—attorneys who specialize in this work charge as much as $1,000 an hour—and the client can bring a cross-claim against the firm to recover its losses. If commercial information is compromised, such as trade secrets entrusted to clients, the related damages also can be significant (e.g., damages in health

care-related cases have run in the millions of dollars).

Cost of compliance with state and federal statutes and regulations. Currently, there are security breach notification laws in 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands. Some require notification to affected individuals and to state authorities. State laws are applicable to residents of a state, so multiple state laws could apply in the event of a data breach. According to a study published by Ponemon Institute, *2011 Cost of Data Breach Study: United States*, the cost per record of a data breach was $194 in 2011. Costs include the average of both direct and indirect costs associated with organizational breaches. The direct and indirect costs cited in the study include forensic investigation, credit monitoring services, customer discounts for future services and products, and loss of business.

In addition to the costs of compliance with state security breach notification laws, the firm may be subject to penalties for violations of federal statutes and regulations. About 50 federal statutes and regulations govern privacy and security. Violations can result in civil and criminal enforcement proceedings. Examples include the FTC Safeguards Rule, as well as the Privacy Rule and Security Rule promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191, and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), P.L. 111-5. Under the HITECH Act, CPA firms with access to individually identifiable health information (e.g., firms processing patient billing records) are subject to civil and criminal penalties for violations of applicable privacy and security rules.

Reputational damage. A privacy breach, actual or perceived, may result in a loss of consumer trust that causes significant damage to the public perception of a firm. That can harm business relationships, especially in the practice of public accounting, which is a business in which trust and confidentiality are critical. Media exposure of privacy-related incidents can lead to significant reputational damage, which, in turn, can result in decreased customer confidence and lost business.

Network damage. Companies of all sizes are at risk for attacks on their computer networks. CPA firms are attractive targets due to their access to data that can be readily sold in the online black market. Intentional hacking attacks aren't the only danger. Malware, which is software designed to impair the operation of various technological devices, can be introduced through email attachments or downloaded software. Malware can disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can also spread out from a firm's system and damage clients' networks. Some malware uses systems to host email spam attacks or to launch denial-of-service attacks.

Insurance coverage applicable to these exposures varies, and firms should understand the coverage parameters of their current policies. Alvin Fennell, vice president of underwriting at Aon Affinity, notes, "Most professional liability policies only cover claims in the course of delivering professional services. Accounting firms should certainly consult with their professional liability insurance carrier to inquire regarding coverage in the event of a breach. If a gap is identified, there may be other products or endorsements from your carrier to cover privacy event expenses."

RESPONDING TO A BREACH

If a breach is suspected or known to have occurred, rapid assessment and damage mitigation are imperative, as outlined below:

Evaluate the severity and scope of the incident. If a laptop computer or other portable device is lost or stolen, identify the data that may have been exposed, and determine whether these materials are protected by password or encryption. Consider engaging forensic information technology experts to determine the scope of the problem. In addition, if the possibility of identity theft or other criminal activity is present, inform appropriate law enforcement agencies of the situation.

Consult with legal counsel regarding compliance with applicable notification laws and public relations activity related to the breach. In addition to laws governing notification of affected individuals and entities, laws governing notification of federal and state regulators must be considered. Share all known details about the breach. Notification requirements vary. Before undertaking any public relations activity, consult with counsel on both applicable law and the best means of managing the situation. Most importantly, do not delay. In the age of social media, a delayed response can result in reputational damage.

Notify potentially affected clients. Most states now mandate notification of customers whose confidential data

may have been exposed. Federal laws also may govern breach notification. Moreover, firms that have experienced a data security breach also may be required to pay for credit monitoring services for potential victims. Some data breach security laws require firms to warn affected persons of the risk of identity theft and fraud within a stipulated time frame, sometimes as expeditiously as within five days. Consider offering potentially affected clients free credit monitoring and identity theft case management services, even if not required by law.

Amy Waldron *(amy.waldron@cna.com) is a risk control consulting director for the CNA Accountants Professional Liability Program.* ***David Hallstrom*** *(david.hallstrom@cna.com) is practice leader for Information Risk Insurance at CNA.*
