Published in: JOURNAL OF ACCOUNTANCY

AICPA® Professional Liability SPOTLIGHT

Controlling your data

August 2016

Use these controls to secure your firm's critical information

By Sarah Beckett Ference, CPA, and Nickolas Graf

Target. Home Depot. Anthem. The IRS. The U.S. government. Numerous hospitals and universities. The commonality? All have been the victims of headline-splashing cyberattacks that led to the breach of confidential data. With so many cyberattacks in the news, many CPA firms may wonder, "Are we next?"

CPA firms can be a treasure-trove of information for cybercriminals. Firms routinely collect sensitive information from both clients and employees, including Social Security numbers, bank account information, earnings and business information, and, if the firm accepts credit cards as payment, credit card numbers. All of this information requires protection under professional standards and various state and federal laws and regulations.

Most firms have acknowledged that data security represents a critical risk requiring careful management. However, implementing controls over data security can be unfamiliar territory with a daunting vernacular. This can be especially challenging for sole practitioners or firms without dedicated IT resources. To help get started, consider implementing these baseline security measures.

RIGHT ACCESS FOR THE RIGHT PEOPLE

Implement access controls to help ensure only authorized individuals are permitted to access sensitive or critical areas or information.

Physical access controls

CPA firms likely restrict access to their premises already, but access to the area in which the firm's server is kept should also be restricted with a lock or access code. If mass storage devices (flash drives, external hard drives, etc.) are used, purchase the encrypted versions. While the cost may exceed that of unencrypted devices, the protection they provide justifies the additional expense. Another option is to use software to encrypt unencrypted flash drives.

Encryption of all laptop and desktop computers and mobile devices is one of the most beneficial controls CPA firms employ. A lost or stolen computer or device can result in a devastating and expensive data security breach if it is not encrypted. Full-disk encryption may help to mitigate damages if a breach occurs. Various state breach notification statutes create a safe harbor that waives notification requirements if encrypted data are breached. Refer to applicable state breach notification laws for information on whether a safe-harbor provision applies.

Full-disk encryption is built into all major operating systems including Windows and Mac OS X. Instructions on how to "turn on" encryption are available online from Microsoft or Apple. BlackBerry devices are encrypted by default as are iPhones and iPads running iOS 8 or newer. The Android operating system supports encryption, but it must be enabled.

Logical access controls

Logical access controls are tools and protocols used for identification, authentication, and authorization of computer information system users, including software programs.

Assign access privileges to software or network folders where sensitive information is stored based upon the principle of "least privilege," meaning a user should only have the minimum access required to perform his or her job responsibilities. Conduct routine reviews of access and modify access authority when an employee leaves the firm, changes roles, or is perceived to be at risk of becoming disgruntled. Many data security breaches are from the inside and perpetrated by a dissatisfied employee or former employee who has knowledge of the firm's systems and their vulnerabilities.

Prepackaged software often comes with default settings. Update the default settings and tailor access rights to your firm. In addition, be sure to implement software updates or patches when they are provided by the vendor. These updates may help troubleshoot and fix a security vulnerability identified and addressed by the vendor.

To help further control access, use passwords. While complex passwords (those that use a combination of upper- and lowercase letters, symbols, and numbers) are good, they are easily forgotten. Instead, focus on long passwords or phrases, 16—20 characters in length, that are changed periodically. Be sure to keep passwords and encryption keys in a secure location. Costly data security breaches have occurred because a password was taped to the bottom of a laptop.

WHAT ABOUT THE DATA?

There are many ways to help protect and manage sensitive information during each step of data flow at a CPA firm.

- **Receiving data.** What kind of information does the firm collect? Does it include information that requires protection? Is this level of information needed to deliver services? Consider whether it could be redacted or modified to remove sensitive information before the firm receives it.

continued…

- **Storing data.** Implement logical access controls on all locations where confidential data are stored, including, but not limited to, servers, electronic storage devices, print drivers, and email servers. Do not overlook physical files. Is client information locked up at night and on the weekend, or are documents left on desks in plain view of cleaning or maintenance personnel? Restrict and secure access to the central filing room or other hard copy file storage.
- **Transmitting data.** Consider how data are provided to and received from clients. If confidential data are sent electronically, send them via an encrypted or password-protected email or, better yet, a secure client portal.
- **Data destruction.** Use a document shredder to destroy old workpapers. If a third-party vendor is engaged to destroy records, ensure it does so in a manner that protects the confidentiality of the information contained therein. Hitting the "delete" button does not permanently delete files from a laptop or mobile device. Electronic records can be permanently deleted individually by using a file-shredding program, or a program can be used to wipe an entire hard drive, permanently deleting all electronic files.
- **Data retention.** Are you maintaining data longer than necessary? Adopt a firm-wide record-retention period, and destroy firm workpapers according to the designated time frame for applicable documents. Evaluate whether applicable law or professional standards recommend different retention periods depending upon the type of information retained. Storage of this data is not only costly but also increases the amount of information that the firm must protect.

USE TOOLS TO KEEP THE BAD GUYS OUT

Many software tools are designed to help prevent or detect intruders in the firm's network.

- **Firewalls** are a primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network based upon specified security criteria.
- **Anti-virus software** is a program or set of programs that is designed to prevent, search for, detect, and remove software viruses and other malicious software such as worms, Trojan horses, and adware.
- Many anti-virus programs include **anti-spyware**, which is designed to prevent and detect unwanted spyware program installations and to remove those programs if installed.

TEST FOR WEAKNESSES AND RESPOND

Conduct regular evaluations of the effectiveness of the firm's data security measures. Testing results can indicate where additional work or training is needed. Good tests include:

- **Ethical hacking or penetration testing.** This is the only time when hacking is good. Certified ethical hackers can help identify potential threats on a computer or network by attempting to bypass the system security and search for vulnerabilities that could be exploited by malicious hackers.
- **Social engineering or phishing.** One of the easiest ways into a firm's network is through an employee. Social engineering schemes have become increasingly sophisticated, involving emails, phone calls, and social media messages that closely resemble those typically received by the employee. The goal is to gain information that can be used to access a system. Often, employees need only to click a link or open an attached file to open the door to hidden malware infecting their device. Conduct tests of employee vigilance by creating and sending false emails or messages to see if employees take the bait.

TRAINING AND VIGILANCE

Data breaches do not always take the form of a cyberattack. The theft or loss of a laptop or flash drive or a misdirected email are common types of data breaches at CPA firms, both of which are preventable. For these reasons, regular security awareness training, constant vigilance, and attention to detail are essential for all firm owners and employees.

WHAT IF A BREACH OCCURS?

Even with these controls in place, a data breach can still occur. Security incidents can take a toll on a firm of any size. Putting an incident or data breach response plan into place can help the firm act quickly, helping to prevent further data loss, regulatory fines, and client backlash.

Sarah Beckett Ference *(sarah.ference@cna.com) is a risk control director at CNA*

Nickolas Graf *(nickolas.graf@cna.com) is a risk control consulting director at CNA. He is a Certified Information Systems Security Professional, Certified Ethical Hacker, and Certified Information Privacy Professional.*

Continental Casualty Co., one of the CNA insurance companies, is the underwriter of the AICPA Professional Liability Insurance Program. For more information, please call Aon Insurance Services, the National Program Administrator for the AICPA Professional Liability Insurance Program, at 800.221.3023 or visit cpai.com.

This article provides information, rather than advice or opinion. It is accurate to the best of the author's knowledge as of the article date. This article should not be viewed as a substitute for recommendations of a retained professional. Such consultation is recommended in applying this material in any particular factual situations.

Examples are for illustrative purposes only and not intended to establish any standards of care, serve as legal advice, or acknowledge any given factual situation is covered under any CNA insurance policy. The relevant insurance policy provides actual terms, coverages, amounts, conditions, and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice.

To learn more about the AICPA Professional Liability Insurance Program, please visit cpai.com or call 800.221.3023

CNA AON