FIRM MANAGEMENT

How Accounting Firms Can Protect Their Data, And Their Clients'

There are several measures CPA firms can take to mitigate data risk and manage their security. CPA firms are responsible for tax identification numbers, social security numbers, financial account numbers, and additional data which can threaten the ...

Patrick Wiley • Jul. 19, 2016

There are several measures CPA firms can take to mitigate data risk and manage their security. CPA firms are responsible for tax identification numbers, social security numbers, financial account numbers, and additional data which can threaten the identity and financial security of clients if compromised.

January 2016's series of cyber-attacks demonstrated the demand for such information when cybercriminals stole Social Security numbers from outside the IRS and used this information to access IRS e-Filing personal identification numbers to file tax returns electronically. One piece of business-critical data can open the doors for hackers to infiltrate a plethora of sensitive files.

Essentially, firms should analyze, implement, and educate when managing its information security. Regular data assessments, proper security planning and implementation, and employee education combine to shield an organization's critical information from cybercriminals.

Here are five steps CPA firms can take to bolster defenses against hackers.

1) Regular security and data assessments

Businesses cannot determine where their network security holes exist without performing a thorough assessment of its security measures and company data use habits. But a single review will not suffice.

CPA firms should regularly evaluate their security strategies and schedule periodic reviews to understand how data is used and stored throughout the organization. Although it may be impossible to fix everything at once, an outlined IT strategy can help safeguard a firm's network and prepare the organization for any challenges that may accompany pending changes.

A CPA firm should evaluate the following aspects of its operations to determine what aspects of its IT environment need to be adjusted.

- Are data security roles assigned to individuals within, or associated with, the organization?
- Are confidentiality agreements in place to ensure the firm's contractors/external entities maintain the organization's security and privacy standards?
- Are regular risk assessments performed?
- Is there a security policy in place?
- Is business-critical data backed up regularly (preferably automatically)?
- Are firewalls and security software in place? Are they updated as needed?
- Where is business-critical data stored?
- How is business-critical data used throughout the organization?
- Who has access to what information?
- What employee off boarding procedures are in place?
- Are employees required to complete regular security and compliance training?
- Is there a formal disaster recovery plan?
- Is there a business continuity solution in place?
- Are compliance standards being met?

2) Technical Security

A majority of business operations occur through the transfer and the use of data and a CPA firm's credibility is based upon its ability to protect this information. Every organization should have a business-grade firewall installed at the forefront of its network. Anti-malware, antivirus, and standard email filtering software are also vital components of a firm's defense against a network intrusion.

Along with sufficient hardware and software, CPA firms should require employees to understand and practice security protocols. Multi-factor authentication, data

encryption, data backup, a disaster recovery plan, and a business continuity solution can help protect a firm against a network breach and allow the organization to continue operations in the face of a data disaster.

3) Physical Security

Even the physical security of a firm's facility can help prevent intruders from threatening its operations and reputation.

Employee key cards, visitor logs, badges, and controlled access to areas where business-critical information is stored enable a firm to monitor and control foot traffic throughout the site. A faulty key card scanner or an open-access data center can leave the organization vulnerable to attack and liable for a number of resulting penalties.

4) Administrative Security

Employee access to sensitive data should align with the individual's role within the organization. As unregulated access to data increases the risk of a network compromise, intentional or not. An employee may accidentally email a sensitive file to someone outside of the organization, thus jeopardizing the security and reputation of the firm. With suitable access controls in place, CPA firms can control who views, edits, and shares data throughout the organization. These controls should be regularly updated to reflect any role changes that occur.

5) Employee training and education

The most vital element of a firm's data security efforts is employee education. An employee's awareness of the methods hackers use to acquire information is critical. If all the protocols and policies are in place and an employee clicks on the wrong website or opens the wrong file because they were enticed by hackers or social engineering phishing attempts, the end result of failing to protect secure data may still result. It's important to frequently educate and update employees regarding security and device best practices. A firm should work to ensure its employees understand protocols such as its BYOD and mobile device usage policies, encryption policies, password policies, and more. The first step toward building a barrier against cybercriminals is helping employees understand the risks involved and how to mitigate them.

CPA firms utilize many forms of technology to store, retrieve and distribute data for both themselves and their clients. It's essential for CPA firms to protect their client's

information as well as their firm's reputation, and these useful and easily-adopted methods can mean the different between data secure and data disaster.

———————

Patrick Wiley is the President and CEO of Aldridge, and has been with the company for 12 years. Wiley is responsible for translating strategic direction into the day-to-day operation of Aldridge. He oversees all aspects of the company's operations, including all services, new business development, finance, sales, legal and human resources. Wiley also leads all of Aldridge's significant mergers and acquisitions activities.

Firm Management • Security • Technology

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.