The Newsletter of the AICPA Private Companies Practice Section

The Risk Management Resource

Provided by Aon Insurance Services

Moving to the Cloud – Everybody's doing it, should you?

You've probably heard about "the cloud" by now. And undoubtedly you've read articles and listened to colleagues espousing the benefits of moving to the cloud. But you may have also heard horror stories about cyber attacks and worry about the security of your client data. Cloud computing offers many benefits to CPA firms. However, there is one critical risk with both legal and ethical implications – protecting the privacy and security of confidential client information. If you move your firm's data to the cloud, how do you know it's protected and secure if you can't see it with your own eyes?

Professional Responsibilities Related to Data Security

Both Rule 301 of the AICPA Code of Professional Conduct and Internal Revenue Code section 7216 require CPAs to protect a client's confidential information and prohibit the unauthorized disclosure or release of such information. Federal and state laws and regulations and state board of accountancy rules may also apply if confidential information is breached. If a CPA uses third party service providers, such as cloud vendors, the CPA is not relieved of the responsibility to safeguard confidential information.

Risk Management Considerations

While nothing is foolproof, there are actions CPAs can take to help protect client confidential information when utilizing cloud vendors, or any third party service provider for that matter.

Perform due diligence

Ethics Ruling 1 of ET §391 states a CPA should "be reasonably assured that the third party service provider has appropriate procedures in place to prevent the unauthorized release of confidential information to others." However, no definition or guidance regarding what is considered 'reasonable' is offered. Utilize professional judgment in making this assessment. Logically, the greater the sensitivity of client information, level of data volume and complexity, or reliance on the cloud vendor, the more thorough the CPA's diligence efforts should be. Areas to consider when making a selection may include, but are not limited to:

- Financial stability of the vendor;
- Vendor's experience working with confidential data and knowledge of applicable regulations and laws, such as the FTC Safeguards Rule, the Red Flags Rule, and the privacy requirements of the Gramm-Leach-Bliley Act and HIPAA;
- Processes and controls to protect CPA firm data and segregate it from data of other users;
- Location of data storage and ability to produce data timely, if needed;
- Vendor's use of third parties to store the CPA's data; and
- Availability of Service Organization Control (SOC) reports issued under the guidance of SSAE No. 16 or other similar framework such as ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

A checklist of considerations when selecting a cloud vendor is provided in the article *Professional Liability Risks Related to Cloud Computing* published by the AICPA Professional Liability Insurance Program. Documentation of diligence procedures performed, results obtained and the CPA's evaluation of the vendor is recommended. Initial and subsequent periodic evaluations to confirm the initial assessment, such as obtaining and reviewing SOC reports annually, are also recommended.

Vendor agreements

Ethics Ruling No. 1 of ET §391 also states the CPA should enter into a written agreement with the third party regarding the maintenance of confidentiality of client information. Agree to key commercial terms with the vendor in writing via a service level agreement or other contract that outlines the terms, services provided by the vendor, metrics by which that service is measured, and remedies or penalties, if any, if the agreed-upon service levels are not achieved. Key contract terms may include:

- Ownership of data – The CPA should be the sole owner of the data.
- Confidentiality of data – The vendor should assume responsibility and legal liability for confidentiality of data.

- Data security breaches – The vendor and CPA's responsibilities related to a privacy breach, including who is responsible for the costs associated with breach investigation, should be clearly defined and understood.
- Notification – The vendor should notify the CPA of breach or other security events within a specific time period.
- Location of data storage – Where the cloud vendor will store the CPA firm's data should be understood. The choice of law provision in concert with laws that may govern the location of data storage should be discussed with an attorney.
- Data outages – Causes of service outages should be addressed in the vendor agreement, including the form and level of compensation and vendor's responsibility to continue service in the event of an outage.
- Maintenance of service levels – The vendor should provide certain levels of service availability and access to data.
- Exit strategy – CPAs should confirm that the vendor will return the CPA's data in a usable format upon termination of the vendor relationship. The vendor should permanently overwrite or delete the data from its servers after returning it to the CPA.

While standard vendor terms are not always negotiable, vendors may entertain reasonable negotiations. The CPA should not blindly accept the vendor's terms and conditions without reviewing them in detail with an attorney to understand risks assumed, or not assumed, by the vendor. If the agreement does not provide the CPA and its clients with the necessary security protections, other vendors or technology resources should be pursued. CPAs should not engage any vendor whose terms would be viewed as "unreasonable" or who attempt to disclaim liability for their own errors, omissions, or neglect.

Tell your client

Ethics Ruling No. 112 of ET §191 and Ethics Ruling No. 1 of ET §391 carve out limited exceptions related to client notification of the use of third-party service providers. However, regardless of circumstance, CPAs should inform clients of the use of third parties and obtain their written consent prior to disclosing confidential information to the third party. A practical means of providing this information is through inclusion of specific language in the engagement letter and in end-user license agreements client portals.

Cover yourself

There are many costs associated with a data breach, including hiring professionals to investigate and fix the breach cause, notification to affected clients, potential fines or penalties, lost billable time and reputational damage, or professional liability claims if the breached information is used maliciously. These costs can quickly add up. Some of the more significant risk exposures include:

- Network loss or damage – costs to restore firm or client networks damaged as a result of exposure to malware, virus or other intentional disruption of computer operations.
- Privacy event expense – costs associated with the investigation of breach cause and notification to affected parties.
- Privacy injury and regulatory expenses – costs related to compliance with state and federal breach notification laws or other applicable privacy law or regulation and damages arising from the data security breach.
- Professional liability claims – damages arising from the malicious use of confidential information breached as a result of the delivery or professional services.
- Business interruption – loss of income and expense incurred to restore operations after a data security breach.

Some of these risks can be mitigated through the use of qualified third party vendors. However, CPA firms remain ultimately responsible for protecting the privacy and confidentiality of data entrusted to them by clients.

Insurance coverage can address these risks. Cyber liability exposures are rapidly changing, and various coverages are available in the marketplace to address them. CPA firms should review current coverages in detail with their insurance agent or broker, and evaluate the need to purchase additional coverage to address these exposures.

Additional Resources

Additional resources regarding the use of cloud computing providers are available here. Some resources require AICPA and/or Information Management and Technology Assurance section membership.

Accountants Professional Liability Risk Control, CNA, 333 South Wabash Ave. 36S, Chicago, IL 60604