Accountant-Client Privilege and the Cloud

Hugh E. Gardenier, III

Abstract

CPAs operate within a complex structure of state accountancy regulations, federal laws, and professional codes of conduct. Paramount to this is the long established responsibility of CPAs to protect and not disclose confidential information received during a professional service engagement without a client's specific consent. The Cloud threatens this principle.

Accountant-Client Privilege and the Cloud

The practice of public accounting in the United States is governed by two key concepts with respect to client data – privilege and confidentiality. This constitutes the research problem and defines the literature review in terms of where and when privilege and confidentiality are applicable. It also delineates circumstances in which activities of or actions against Cloud Service Providers (CSPs) could result in data breaches which violate privilege and confidentiality. For purposes of this paper actions of the CPA are dependent variables and the actions of and to CSPs are independent variables.

Clients assume and expect that conversations with their CPA constitute privileged communications, and as such, the matters discussed will not be disclosed to third parties without client approval. Along with this, client data and information is confidential and disclosure also requires client consent. Federal courts, however, have routinely rejected the idea of accountant-client privilege and such privilege is not protected by common law (U.S. v. Arthur Young & Co., (1984), National Union Fire Ins. Co. of Pittsburgh, Pa. v. KPMG Peat Marwick (1999)).

Accountant-client privilege, nonetheless, is covered by statute in twenty-five states, (Beardslee, 2009, p. 36) and dependent upon the scope of the administrative and occupations codes in the state, includes a range of testimonial and confidentiality privileges which are only applicable to state courts in that jurisdiction (Causey and McNair, 1990, p. 539). Moreover, confidentiality of client data is addressed in the CPA’s ethical duties and is covered by the AICPA’s Code of Professional Conduct and conforming bylaws in individual state CPA societies. The CPA using the Cloud is bound by the Code of Professional Conduct to protect and preserve client data regardless of whether it is stored in their file room or on a Cloud server in India.

The literature review is divided into four primary categories which are designed to develop the concept of privilege —– where privilege might be asserted; a general processing framework and traditional business model for tax services; the evolving area of data security and information assurance; and legal issues unique to the Cloud. Tax services are used as an example because of greater outsourcing and online development in this practice area.

Accountant-Client Privilege

As defined in the introduction, the existence, scope and extent of accountant-client privilege is dependent upon the state in which a CPA is licensed and practices. In at least twenty-five states the loss of privilege or the breach of confidentiality could represent a significant legal problem for CPAs in the event of misuse of Cloud resources by users, unauthorized third parties, or law enforcement. This is an emerging legal issue and in order to determine legal activity in this area a text search of state cases at the appeals court level for all fifty states was performed using Westlaw. Using the search term "accountant-client privilege," 145 cases were identified.

The table below identifies by state the frequency of case occurrence. The standard deviation of these cases was 5.11. Seven states — Colorado, Florida, Georgia, Indiana, Maryland, Michigan, and Pennsylvania — were more than one standard deviation from the mean of 2.9 cases, and aggregated 95 cases, or 65.5 percent of all cases identified. These states were considered to be statistically significant for analysis purposes and represented a higher likelihood, based upon cases on appeal, of the principle of accountant-client privilege being asserted in a state court. State court cases are relevant to this analysis because: (1) Federal courts do not recognize accountant-client privilege, and (2) while there is a uniform CPA exam, there is no nationwide practice license for CPAs. CPAs are licensed by individual states and are subject to occupational and administrative codes in those states. These seven states represent "hot-beds" for asserting accountant-client privilege, and by correlating state CPA license data in each of these seven states with the number of state accountant-client privilege cases it is possible to efficiently direct further legal research.

State	Number of Cases	State	Number of Cases	State	Number of Cases
Alabama	0	Alaska	1	Arizona	6
Arkansas	0	California	3	Colorado	11
Connecticut	1	Delaware	5	Florida	28
Georgia	9	Hawaii	0	Idaho	1
Illinois	4	Indiana	9	Iowa	0
Kansas	2	Kentucky	1	Louisiana	2
Maine	0	Maryland	15	Massachusetts	0
Michigan	10	Minnesota	0	Mississippi	0
Missouri	5	Montana	0	Nebraska	0
Nevada	3	New Hampshire	0	New Jersey	1
New Mexico	0	New York	3	North Carolina	2
North Dakota	0	Ohio	1	Oklahoma	0
Oregon	0	Pennsylvania	13	Rhode Island	1
South Carolina	0	South Dakota	0	Tennessee	2
Texas	2	Utah	0	Vermont	1
Virginia	3	Washington	0	West Virginia	0
Wisconsin	0	Wyoming	0		

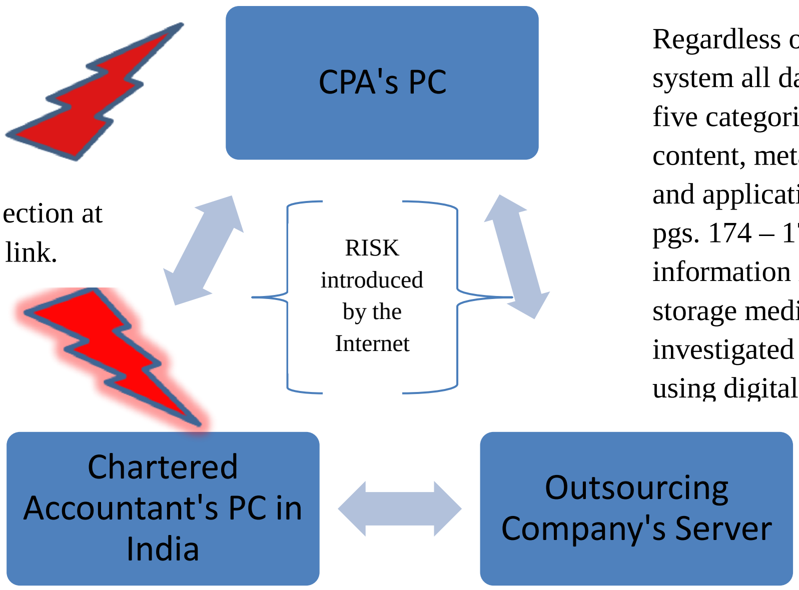
Table 1: "Accountant-Client Privilege" Cases by State

Traditional Outsourcing and Confidentiality

In accordance with the AICPA's Code of Professional Conduct [ET Section 301.01], "a member in public practice shall not disclose any confidential client information without the specific consent of the client." On the surface this rule could preclude the use by CPAs who belong to the AICPA (members), of some offsite, third-party service providers that provide a range of administrative support and data processing services, or at a minimum require the disclosure of such service providers to clients. Brody, Miller and Rolleri addressed this in December 2004 with respect to the outsourcing of tax return preparation by CPAs to tax preparation companies in India (Brody, Miller and Rolleri, 2004, pg. 12). This is significant because the outsourcing of tax return preparation was a precursor to the offshoring of accounting data in the Cloud. At the time of their study approximately 200,000 U.S. income tax returns were being prepared annually by outsourcing firms claiming to employ Chartered Accountants in India. Since 2004 the number of tax returns being outsourced has grown exponentially and has been estimated to be well in excess of 1.6 million returns in 2011 (Cervantes, 2009, pg. 104).

Outsourcing transaction flow is represented as being secure via Internet connections to a third-party service provider in the United States with retransmission of client tax information to a preparer company in India. Processors utilizing this business model have represented that their security engineering and information assurance measures are superior to those utilized in the backroom operations of most CPA firms. In actuality, the transmission of any client data outside the physical confines of a CPA's office via the Internet provides a digital trail which can be investigated by law enforcement, and exploited by disgruntle employees, blackhats (hackers), unethical competitors, and unauthorized third-parties (Figure 1).

Security and information assurance issues attributable to this outsourcing model have been primarily delegated to service providers similar to CSPs. The AICPA addressed ethical issues of outsourcing professional services in ET sec. 112 par. 224-225, stating "before disclosing confidential client information to a third-party service provider, a member should inform the client, preferably in writing, that the member may use a third-party service provider." Nonetheless, this ethics interpretation may be misconstrued by CPAs because the AICPA goes further and states "a member is not required to inform the client when he or she uses a third-party service provider to provide administrative support services (for example, record storage, software application hosting, or authorized e-file tax transmittal services) to the member." This ethics ruling may not provide a safe harbor for the more complex application of outsourcing of services to CSPs. Unintentional disclosure of confidential client information via a Cloud data breach has not been addressed by the AICPA, nor has it been sufficiently addressed in terms of the impact on accountant-client privilege. In 2003, Pacini, Seay, and Placid addressed the issue of inadvertent disclosure of client information by accident or eavesdropping when client information was transmitted via electronic communication. This discussion was pre-Cloud and the technology was limited to cell phones, cordless phones, faxes, and email (Pacini, Seay, and Placid, 2003, pg. 1)


CPA's PC
RISK introduced by the Internet
Chartered Accountant's PC in India
Outsourcing Company's Server

Regardless of the operating system all data is maintained in five categories: file system, content, metadata, file name, and application (Carrier, 2005, pgs. 174 – 178). This information is maintained on storage media and can be investigated on-site or remotely using digital forensics methods.

Malware injection at the weakest link.

Circumventing of security controls can result in the loss of client data files, and unauthorized transfer of client information such as social security numbers. Control environment may not be as secure as that provided by organizations servicing multi-national financial services companies.

Client files being processed are stored on the outsourcing company's server hard drive(s). File fragments typically remain in slack space on the drive and may include user names, passwords, information from system memory, and other sensitive data even after the data files are deleted. (Cardwell, etal, 2007, pg. 495).

Figure 1 - Loss of Privilege Through Data Breaches

The Impact of Cloud Computing on the Traditional CPA Business Model

Cloud computing represents the evolution of data communications networks (Shelly, Cashman, 1980, pgs. 8.1 – 8.31). While traditional service bureau – user relationships have been static, Cloud services are dynamically scalable and allow users to use a Web-based platform in three common configurations: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS) (Jensen, Schwenk, Gruschka, and Iacono, 2009, pg. 1). In theory this provides the user the opportunity to define an IT environment that is most conducive to their business model. As defined in marketing literature, the Cloud promises the opportunity for CPAs to:

- Significantly cut IT costs by cutting back or even eliminating in-house data centers and IT staff
- Increase data security by providing remote backups of data
- Eliminate the worry of application program patches, security updates, and patches
- Increase staff productivity and redirect resources to core enterprise purposes
- Scale IT service and work on a “pay-as-you-go” basis thereby avoiding large capital investments in computer equipment and software

These are attractive attributes and in an economic environment with a revenue stream that is highly susceptible to recession and competitive pressures, CPAs are being aggressively pitched Cloud services by major providers of accounting services software. The provision of these Cloud services does not take into account the unique position of the CPA in providing professional services, or the implications of accountant-client privilege when confidential client data is spread across remote servers in multiple countries not subject to U.S. law.

Data Security, Information Assurance, and Legal Issues Unique to the Cloud

Cloud-based services challenge any business based upon: (1) commingling of data in a virtual machine environment with hard drives not being segregated by customer, therefore allowing virtual hard drives to span several servers; (2) geographic boundaries of Cloud servers not being readily determinable; (3) data backups being outsourced to third-party providers frequently located outside the United States; (4) data in many instances being subject to multiple state, federal, and international jurisdictions; and (5) the quality of all service being based on the continuity and quality of an Internet connection. All of these Cloud characteristics increase the probability that privilege can be lost through accident or by intent.

Perhaps of more concern, however, is compliance with E-discovery requests which vary widely from country to country. While in the United States, discovery is generally governed by either the Federal Rules of Civil Procedure or the applicable state rules of civil procedure, many countries including France, Germany, Spain, and the Netherlands have filed under Article 23 of the Hague Convention on Evidence declaring “that discovery of any information, regardless of relevance, will not be allowed if it is sought in relation to foreign legal proceedings” (Lillard, Garrison, Schiller, Steele, and Murray, 2010, pgs. 288 -293). In this backdrop it is not beyond imagination that a CPA can find themselves or their client facing legal sanctions because it is impossible for them to comply with discovery because of where their Cloud server is domiciled. This is a parallel world from that described by proponents of the Cloud, and in many respects users are like Alice attempting to have a coherent conversation with the Queen:

“The rule is, jam tomorrow, and jam yesterday – but never jam today.”

“It must come sometimes to ‘jam today,” Alice objected.

“No, it can’t,” said the Queen.

"It's jam every other day: today isn't any other day, you know." (Carroll, 1999, pg. 196)

At a time when IT spending for internal projects shrank in most industries, IT spending for Cloud computing services exploded. This growth, as identified by Gartner Inc., increased by 20 percent between 2008 and 2009 to $56 billion, and by 2013 this spending is estimated to grow another 132 percent to $130 billion. (Rhoton, 2011, p.3) While many of the players in Cloud computing are well known companies such as Amazon, AT&T, Cisco, Citrix, Google, HP, IBM, Microsoft, Novell, and Oracle, the majority of providers weren't in existence ten years ago (http://cloudcomputing.sys-con.com/node/770174, October 29, 2009). Aggressive marketing of these services has resulted in an IT environment that is perceived by many users to be more secure than existing in-house systems, but the reality is just the opposite. Gartner Inc., in a March 2010 press release, noted that "60 percent of virtualized servers will be less secure than the physical servers they replace through 2012," and that 30 percent of virtualized servers will still be insecure as of 2015 (http://www.gartner.com/it/page.jsp?id=1322414, March 15, 2010).

This is apparent when consideration is given to recent hacking attacks on Cloud-based networks. Distributed Denial of Service (DDoS) attacks have evolved and have become coldly calculating in forcing Cloud servers to crash, hang, or reboot. This is normally accomplished by using the services of a less secure decoy network, taking control of that network, and then using all the resources of that network to attack a target system. In this manner, what would normally be a DoS attack on a target system by one PC, could become a highly-coordinated attack on a target system by thousands of PCs at one time (Fadia, 2006, pgs. 542 - 544). When a decoy network is not available, creation of a network solely for the purpose of malicious intent can easily be done. Bot-ware, which is frequently unknowingly installed by users through social engineering ploys, hides in rootkits and communicates with a bot-master in a central network, creating a silent army of zombies that can be unleashed on a single target without warning (Dr. K, 2008, pgs. 174 – 177). A more sinister attack scenario with respect to CPAs using the Cloud is a Fraudulent Resource Consumption (FRC) attack. An FRC attack consumes application resources and bandwidth in a fraudulent manner.

Many CSPs use a utility pricing model whereby the total cost of computing in the Cloud is determined by:

Total Cost = Cost-Per-Hour (Hours) + Cost-of-Data-Transferred (Bytes)

This pricing model is beneficial because it avoids large start-up costs. In this scenario a bot-net could be used to attack application layer resources by means of HTTP flooding attacks (Idziorek and Tannian, 2011, pgs. 33 – 37). This type of attack is particularly viable when a CPA firm uses a Cloud server to maintain a Website and as a portal for client data transfer. The result is an attack duration that could last weeks or months, with bandwidth used steadily rising and per transaction costs becoming prohibitive. Since the CPA firm does not maintain Cloud server logs, this would only become identifiable through the billing records of the CSP. This type of attack has been used by at least one online merchant to flood competitors' websites and disrupt online transactions (Ranjan, Swaminathan, Uysal, and Knightly, 2006, pg. 1).

Threat analyses and the vulnerability of data centers containing Cloud servers is not widely discussed or appreciated in the public accounting environment, and is not quantified in an environment where attorney-client-accountant privilege could be breached through the loss of privileged documents or confidential data. Bodin, Gordon, and Loeb have written widely on information assurance topics and in 2008 suggested the use of the Analytical Hierarchy Process (AHP) in order to calculate the expected loss from a data breach (Bodin, Gordon, and Loeb, 2008, pgs. 64 – 68). This process requires the decision maker to estimate the magnitude of a loss necessary to threaten the survival of the organization. Determining this projected loss in an environment where the CPA does not have control over the CSP is extremely problematic.

Other writers have identified risk based upon the type of system involved, the source of threats, and intended behavior of the attacker in a threat environment. Thus, while a cyber-attack on a power plant may have serious primary and secondary results which can be quantified in terms of economic damages, an attack on a CPA’s CSP may have long-term implications that can’t be readily quantified. In this manner, international standards which recognize six levels of threat instantiation likelihood provide a good starting point for determining the frequency of threat occurrence (Herrmann, 2002, pg. 86).

1. Frequent – frequent occurrence with an expectation of 1 in 100 times
2. Probable – this can be expected to happen 1 in 1,000 times
3. Occasional – likely to occur 1 in 10,000 times
4. Remote – likely to occur 1 in 100,000 times
5. Improbable – unlikely to occur, but with an expectation of 1 in 1,000,000 times
6. Incredible – extremely unlikely to occur, but with an expectation of 1 in 10,000,000 times

While frequent to occasional threats might entail common power outages, issues with Internet connectivity and local equipment malfunctions, remote to incredible threats should be considered to have a higher likelihood to occur when bot-nets and Cloud server resources are used to coordinate DDoS attacks, thereby increasing the number, magnitude and duration of individual threats. As seen in the spring 2011 Sony PlayStation Network attack, which reportedly compromised the data of seventy million users, knowledgeable users using scalable, virtualized servers can easily crack password protected systems utilizing the near-supercomputer power from readily available CSPs.

These data breaches are significant both in terms of the small amount of resources used to successfully attack sophisticated, well-managed and capitalized service providers, and in the broader implication with respect to CPAs who may be relatively unsophisticated users using Cloud computing services based upon “marketing assurance of suitability” without an understanding of their data security, legal, ethical, and business continuation risks.

Perhaps more disturbing is when law enforcement becomes the threat. In the case of Liquid Motors, a Dallas based company providing inventory management and marketing services for more than 750 auto dealers nationwide, this became a nightmare that was all too real. When FBI agents raided the offices of Core IP Networks and seized all data servers, including those storing Liquid Motors’ data, it put Liquid Motors out of business for a period of time. Liquid Motors was not being investigated, but since data is co-mingled on multiple virtual servers, the agents had to seize all servers to make mirror images of the data. Liquid Motors eventually had their data returned after providing hard drives to the FBI, but the down time and damage to their business and their reputation was significant (http://www.wired.com/threatlevel/2009/04/company-caught/, April 8, 2009).

Not to be ignored is the substantial economic risk CSP users face. What happens to a CPA’s data if the data center files bankruptcy, goes out of business or the data communications infrastructure collapses under the weight of regional financial distress?

Proposed Data Collection Methods

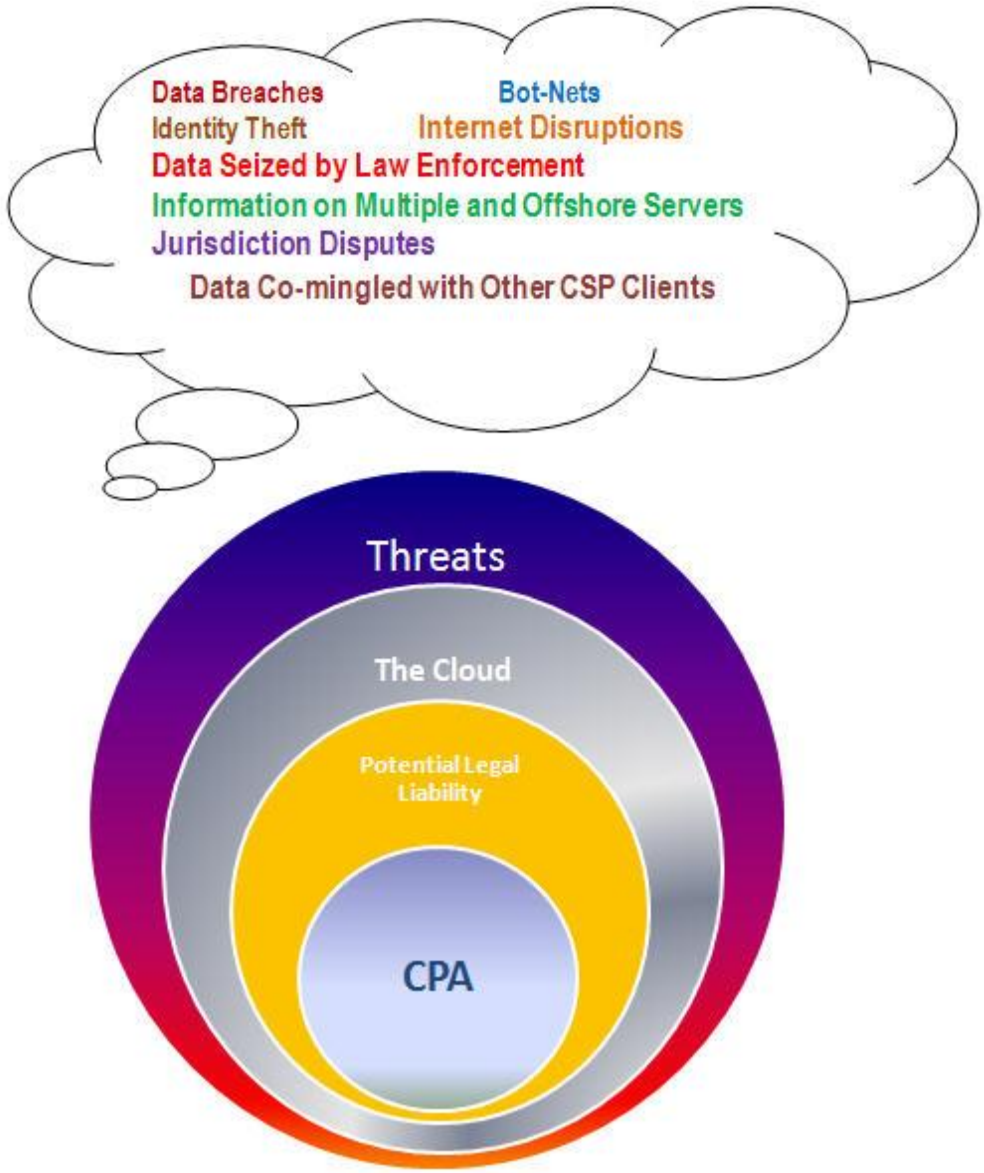
The research problem at hand is maintaining privilege and confidentiality of data when CSPs are used by CPAs in public practice. This defines our problem in terms of unintentional data breaches where an undeterminable data loss occurs. The actions of the user (the CPA) in identifying the threat before the data breach occurs and in mitigating damages after the fact constitute the dependent variable. The user has very little control over independent variables which primarily consist of data security controls and external risk factors attributable to the threat environment the CSP operates in.

While the public accounting profession in the United States has largely become risk-based in the providing of attest services, this analysis process has not carried over to the assessment and quantifying of risk incurred by CPAs when they migrate to the Cloud. In the extreme, common sense dictates that risk assessments should be multi-dimensional and that no one risk model can fit all practice scenarios. But in performing the literature review no published studies documenting the impact of Cloud services on CPAs and their perception of such services were identified. Anecdotal information was available in abundance from service providers who champion the use of Cloud services, but there has been no objective evaluation of the needs of middle-market public accounting firms, the technical abilities of those users, and a well-structured analysis of those services in the academic press. Of particular note, the AICPA, which presents itself as an advocate for the profession, through its CPA2Biz subsidiary has released a series of case studies which enthusiastically promote the use of Cloud services, but fail to mention even basic data security and information assurance considerations (CPA2Biz, 2011, LarsonAllen; CPA2Biz, 2011, N. Cheng & Company; CPA2Biz, 2011, CPA2Biz, 2011, XBS Global; CPA2Biz, 2011, SS&G). This, of course, raises issues of objectivity and increases concerns with respect to the application of ET sec. 112 par. 224-225.

In addressing the problem, defined dependent variables can be tested by circularizing CPAs in public practice in order to develop a baseline for development of a risk-based Cloud adoption model. Information obtained from the literature review of the four primary categories addressed in this paper will constitute the survey framework with the survey being administered using the resources of a subscription service, SurveyMonkey.com. The survey will be available to participants by clicking a URL address provided to participants on the Internet. Solicitation of responses will be encouraged by listings on business oriented, CPA networking websites on the Internet (LinkedIn), social-media websites (Facebook) dedicated to the profession and direct contact with university accounting departments. Survey questions will be designed to address eight key areas:

1. Education of respondents
2. Professional experience
3. Practice size
4. Areas of practice
5. Continuing education applicable to Cloud computing
6. Exposure to and knowledge with respect to Cloud computing
7. Understanding of the concept of accountant-client privilege
8. Geographic region and size of community where the public practice is located

Survey results will be correlated to provide a profile of CPAs by geographic location, professional experience, and understanding of Cloud computing services. From this data a risk-based model for implementation and use of Cloud computing services by CPAs will be developed.


Data Breaches
Bot-Nets
Identity Theft
Internet Disruptions
Data Seized by Law Enforcement
Information on Multiple and Offshore Servers
Jurisdiction Disputes
Data Co-mingled with Other CSP Clients
Threats
The Cloud
Potential Legal Liability
CPA

References

AICPA Code of Professional Conduct (2011), “Use of a Third-Party Service Provider to Assist a Member in Providing Professional Services,” ET sec. 112 par. 224-225, May 31, 2011.

Beardslee, Michele D. (2009), “The Corporate Attorney—Client Privilege: Third-Rate Doctrine for Third-Party Consultants,” SMU Law Review, Spring 2009.

Bodin, Lawrence D., Gordon, Lawrence A., and Loeb, Martin P. (2008), “Information Security and Risk Management,” Communications of the ACM, Vol. 51, No. 4, April 2008.

Brody, Richard G., Miller, Mary J. & Rolleri, Michael J. (2004), “Outsourcing Income Tax Returns to India: Legal, Ethical, and Professional Issues,” The CPA Journal, December 2004.

Cardwell, Kevin, etal (2007), The Best Damn Cybercrime and Digital Forensics Book Period, Syngress Publishing, Inc., Burlington, MA.

Carrier, Brian (2005), File System Forensic Analysis, Addison-Wesley/Pearson Education, Inc., Boston, MA.

Carroll, Lewis (1999), The Annotated Alice: The Definitive Edition (Hardcover), W.W. Norton & Company, New York, NY.

Causey, Denzil & McNair, Frances (1990), “An Analysis of State Accountant-Client Privilege Statutes and Public Policy Implications for the Accountant-Client Relationship,” American Business Law Journal, Vol. 27, 1990.

Cervantes, Paul (2009), “Sarbanes-Oxley and the Outsourcing of Accounting,” The Michigan Journal of Business, Vol. 2, 2009.

CPA2Biz, “LarsonAllen Moves to Migrate Its Outsourcing Clients to Intacct,” Intacct Accountant Edition, 2011.

CPA2Biz, "N. Cheng & Company Uses Intacct to Improve Service to Non-Profit Clients," Intacct Accountant Edition, 2011.

CPA2Biz, "XBS Global Expands Their Business Consulting Services with Intacct," Intacct Accountant Edition, 2011.

CPA2Biz, "SS&G Grows Their Business More Than 75% in One Year with Intacct," Intacct Accountant Edition, 2011.

Dr. K, (2008), Hackers' Handbook 3.0, Carlton Books, London, UK.

Fadia, Ankit (2006), The Unofficial Guide to Ethical Hacking, Thomson Course Technology, Boston, MA.

Gartner, Inc. (2010), "Gartner Says 60 Percent of Virtualized Servers Will Be Less Secure Than the Physical Servers They Replace Through 2012," Gartner Newsroom, http://www.gartner.com/it/page.jsp?id=1322414, March 15, 2010.

Goodman, Christopher J. & Mance, Steven M. (2011), "Employment loss and the 2007-09 recession: and overview," Monthly Labor Review, April 2011.

Herrmann, Debra S. (2002), Security Engineering and Information Assurance, Auerbach Publications, New York, NY.

Jensen, Meiko, Schwenk, Jorg, Gruschka, Nils, & Iacono, Luigi Lo (2009), "On Technical Security Issues in Cloud Computing," 2009 IEEE International Conference on Cloud Computing, 2009.

Ranjan, S., Swaminathan, R., Uysal, M., and Knightly, E., (2006), "DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection," INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings-April 2006 Barcelona, Spain.

Shelly, Gary B., Cashman, Thomas J. (1980), Introduction to Computers and Data Processing, Anaheim Publishing Company, Brea, CA.

SYS-CON Media Inc. (2009), “The Top 150 Players in Cloud Computing,” Cloud Computing Journal, http://cloudcomputing.sys-con.com/node/770174, (October 29, 2009).

U.S. v. Arthur Young & Co., 465 U.S. 805, 104 S. Ct. 1495, 79 L. Ed. 2d 826, 15 Fed. R. Evid. 742 So. 2d 328 (Fla. Dist. Ct. App. 3d Dist. 1999), decision approved, 765 So. 2d 36 (Fla. 2000)

Zetter, Kim (2009), “Company Caught in Texas Data Center Raid Loses Suit Against FBI,” Wired, http://www.wired.com/threatlevel/2009/04/company-caught/, April 8, 2009.