Cloud Computing: Proceed With Caution

By Brian Tankersley, CPA.CITP

The technology industry is going through a disruptive change. Many futurists predict the data and applications which are stored and run from our local computers will migrate to massive data centers connected to the internet over the next ten years. The computer hardware used to access these server farms will not store or process data, but will instead act as a terminal into this massive network, or “cloud” of resources. Applications and data which hosted online and rented instead of purchased are described as “Software as a Service,” or “SaaS”, and are also referred to as “cloud computing”. Web and cloud-enabled applications can let you share information with a team of professionals across the globe in real time, and gives any organization world-class security professionals using state of the art data centers which are designed to provide both application availability and data security. The leaders in the space include major players such as SalesForce.com, Intacct, NetSuite, Intuit’s ProLine applications, CCH’s ProSystem fx, and Thomson Reuters’ Workflow and Software Solutions product lines, but also include specialized SaaS providers such as Braintree-based XCM Solutions, Andover-based Copanion, Accountants World, and audit confirmation provider Capital Confirmation.

While there are many new benefits associated with this new computing module, there are also many new risks which need to be managed and mitigated. These risks can be classified into three major categories:

- Security and Privacy,
- Availability of Applications and Data, and
- Compliance with Laws and Regulations.

Accountants should perform adequate due diligence on any “web-based” or “cloud-based” software to make sure these offerings, as deployed and implemented, will meet all current and future requirements for service and data availability, privacy, and legal/regulatory compliance. Organizations should continue to prepare and test backup service plans and alternate providers in the event of serious problems such as service interruption, provider shutdown, or a privacy breach.

**Security and Privacy**

When most accountants think of cloud computing initiatives, they are immediately concerned with security and privacy, since SaaS involves storing confidential information on remote servers. In many cases, data center hosted solutions can offer better security than can be implemented in many small and mid-sized businesses, often with lower capital and operating costs. Cloud application providers typically host applications in hardened data centers, with multiple layers of physical security, as well as redundant power supplies, internet connections, and hardware. In contrast, many small business server infrastructures are only protected by a door on an unlocked closet in the office, making them vulnerable to theft using “smash and grab” techniques, weather issues, and many other threats.
Since most physical security concerns are handled by application service providers, end users must focus their efforts on ensuring strong authentication methods are used to gain access to applications and data. The potential for exposure due to a breach of data security is more significant in a SaaS environment, since outsiders can execute malicious internal and external attempts for unauthorized access to data with impunity by guessing usernames and passwords. While the physical security of a personal computer with locally installed applications in a locked office may somewhat compensate for the weak logical security associated with an easily guessable password, the same weak password in a SaaS environment can easily lead to a privacy breach.

SaaS applications also have additional risks associated with the privacy policies established by providers which govern how and where information can be disclosed to third parties. Many of these privacy policies are subject to change by the service provider without notice to the subscriber. In most cases, these agreements should also be reviewed with an organization's legal counsel before confidential information is stored on remote systems. End users of SaaS applications may also not have legal standing to quash overly broad subpoenas issued by a plaintiff or governmental agency, and may be legally prohibited from disclosing the event to the end user. Accordingly, users should exercise due professional care and consult relevant experts as part of the evaluation process.

**Availability of Applications and Data**

A second area of concern surrounding SaaS applications is the availability of hosted applications and related data. Events such as fires, storms, cuts in fiber optic cabling, sun spots, and hardware failures can result in unexpected downtime for any computerized applications. Providers can go bankrupt, resulting in downtime and possible breach of security over confidential information. Many service contracts allow the provider to disable or delete free accounts and all related data without recourse, so users of those services may want to back up their personal information to local systems as part of their business continuity strategy. Service contracts may be referred to as “End User License Agreements”, or EULAs, “Terms of Service”, or TOS, and “Terms and Conditions”. These risks should be considered and evaluated before deploying SaaS applications.

The infrastructure needed to support SaaS applications may be available in every location. Organizations who have unreliable internet connections or who cannot get a fast, low-latency broadband internet connection may not be a good fit for SaaS deployments. Companies with significant SaaS deployments should strongly consider multiple internet connections (e.g. cellular, cable, fiber, T-1, or DSL) so staff can access SaaS applications even when one provider is down.

Businesses should also investigate the service level agreement (SLA), uptime guarantee, or terms associated with their internet service provider. A cable internet user on a home internet connection might report interruption on Monday and have a technician in their home on “Friday, sometime between 1:00 and 5:00 PM”. If uptime from a home office is a concern, home users should invest in a more expensive business grade internet connection, which could have an SLA which generally requires a much more rapid response to service failures.

Businesses should also have a clear plan for how they will implement the solution, and how they will retrieve their data if they ever discontinue the use of a particular service before they make any commitments. Without a well developed exit strategy, users may have to reperform many tasks on historical data when they transition to a new solution. Many providers have excellent resources to assist in this effort. For example, Google offers an excellent website (www.dataliberation.org) which gives instructions on how users can import their existing data into Google’s applications, as well as directions for downloading and removing their data if the user ever decides to discontinue service.
Compliance with Laws and Regulations

One of the most challenging areas associated with using hosted applications and SaaS is compliance with applicable laws and regulations. While the regulations themselves may require some configuration changes and user education (e.g. using secure portals instead of e-mailing confidential information), simply knowing what rules apply and whose rules govern a situation can be very difficult. A partial list of laws and regulations where accountants may have exposure include:

- Health Insurance Portability & Accountability Act (HIPAA)
- American Recovery & Reinvestment Act of 2009 (ARRA)
- Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLB)
- Federal Education Records Privacy Act (FERPA)
- IRC § 7216 and related regulations
- Payment Card Industry Data Security Standard (PCI)
- European Union Data Privacy Directive

Federal contractors and agencies may be subject to additional regulations from the National Institute of Standards and Technology (NIST) and other agencies.
Statutes in Massachusetts and other states where you do business, including 201 CRM 17.0, Mass. Gen Laws § 93H-1 et seq, N.H. Rev. Stat §§ 359-C:19 to C-21, and many others. State laws governing confidentiality, such as those covering employer-employee, accountant-client, and lawyer-client relationships.

For example, a tax practitioner in Massachusetts who accidentally sends all K-1’s to each of the 500 partners in a REIT instead of sending each partner their individual K-1 might be required to report the breach using procedures promulgated by each of the 46 individual state statutes, depending on where the partners are incorporated, where they live, or where they retrieve the e-mail message. If the secure portal was stored on a server in another country without proper disclosure to the taxpayer or redaction, it could be a violation of regulations under IRC § 7216.

Figure 2 - Google Docs makes no promises on compliance issues for accountants like HIPAA, GLB, and IRC §7216

The difficulty of complying with laws and regulations can be made more difficult by provider policies about stating compliance or non-compliance with specific regulations. One example of a provider who will not take a position on their services’ compatibility with most security statutes is Google, who responds to questions of HIPAA and FERPA, in part, with the following statement:

“...Generally, an organization must decide whether its use of our products is compliant with any regulations the company may be subject to.”

The legal environment for privacy and identity theft statutes has changed radically in the recent past. In 2002, there were few, if any, state laws which directly addressed security and identity theft management. The first state statute was passed in California in 2003, and at least 45 additional states have created similar statutes in the last seven years. Some of the state laws include provisions such as fines, imprisonment, tort liability, and public reporting for failure to fully comply with their

---

requirements. Every accountant should have a basic knowledge of the laws they are required to follow, and should consult legal counsel if questions arise.

**Conclusion**

Although SaaS solutions offer significant opportunities for accounting professionals, users should have a clear understanding of the security, privacy, application and data availability, and compliance requirements. Users should also have clear plans for how they will transition into and out of the service before they implement, and should revise their plans continually as service offerings change. While no plan can prevent every possible source of downtime or information breaches, a well-thought out plan, created in consultation with relevant experts, can help users realize the benefits of SaaS while effectively manage the associated risks.

Brian Tankersley is a CPA and CITP based in Knoxville, Tennessee. Tankersley teaches continuing education courses with MSCPA through K2 Enterprises, writes a regular column for the CPA Technology Advisor, publishes a recognized accounting technology blog (CPATechBlog.com), and is a senior faculty member with Becker Professional Education. Tankersley can be contacted by e-mailing brian@bftcpa.com.