Considerations when Entering into Cloud Computing (SaaS) Contracts

Kara Bufalino  
November 25, 2015

Software as a Service, or “SaaS,” is part of what is known as “cloud computing.” It is quickly becoming a desirable option for many companies because of the lower up-front costs and ease of access. SaaS delivers technology applications via the Internet where data is inputted, stored and accessed remotely. This avoids the capital-heavy expenses of installation and maintenance of an on-premises IT infrastructure. It also allows for a quicker and more efficient way to update the software and troubleshoot any potential problems that arise. Although the benefits may appear to make SaaS an easy choice, there are potential pitfalls that can cause major harm to a company that need to be taken into consideration.

SaaS vs. the End User License Software Model

A company traditionally acquires software through a subscription-based model where the software provider grants a license to the end user. This approach is typically done through a software license agreement and usually comes with a hefty licensing fee to be paid up-front. In contrast, SaaS payment terms are on a subscription basis where the cost is spread out over a longer period of time. Additionally, due to the “remote” nature of SaaS, the data is no longer stored on the premises of the business, allowing the data to remain protected if some sort of disaster were to occur at the business. Further, in contrast to the manual updates that can cut down on the efficiency of a business, SaaS provides only the most current version. Ultimately, SaaS can be a desirable option for companies that may be short on capital and do not want to be stuck with out-of-date software. However, there are certain risks that must be weighed before a company decides to replace its usual end user-licensed software with SaaS.
Issues with SaaS

The following provides a brief overview of the issues that should be considered in conjunction with SaaS:

**Security:** If sensitive company data and business processes are to be entrusted to a third-party service provider, then issues such as identity and access management will need to be addressed. Additionally, companies must be aware that data can be accessed while in transit over the Internet, or on the remote server where it is stored, thus making it vulnerable.

**Limited Software Choice:** Instead of being able to continue using a tried-and-true version of software, with SaaS, businesses only have access to the most current versions.

**Payment of Subscription as Necessary for Continued Service:** In contrast to the end user license agreement which allows the end user unfettered access once the license fee has been paid, a company that utilizes subscription-based SaaS services must continue to pay — even when the service is poor or the software has bugs — in order to maintain access.

**Potential for Hidden Costs:** When reviewing the contract from a SaaS provider, it is crucial to take note of what exactly is covered by the subscription fee. In many instances, there are additional costs for configuring and setting up the software, as well as for installing the software on certain devices such as smart phones and tablets.

**Questionable Data Rights:** There exists much ambiguity on whether the right to access the data remains with the customer and, more importantly, what rights the SaaS provider has to the data that is being stored on its system.

**SaaS Contract-Specific Points**

Once a business chooses SaaS, special attention must be paid to the agreement provided by the vendor. Although larger SaaS vendors will have form agreements that offer little room for negotiation, it is still important to keep the following provisions in mind while reviewing:

**Subscription Price:** It is important to review what exactly is included in the subscription. In many instances, integration, client training and support are the responsibility of the client, and receiving such services from the vendor will require additional costs.

**Performance:** Service Level Agreements are becoming more common in SaaS contracts — these agreements usually provide guarantees on when service will be available (known as “uptime”). Additionally, it is important that there be language requiring the obligation of the vendor to perform regular back-ups. Further, if possible, it is smart to include a provision that provides the client with the right to receive a credit, or in the best case scenario — a right to terminate, upon the occurrence of any service lapses.

**Privacy and Security:** The contract should set forth specific procedures to follow in the event of a data breach, disaster recovery, or termination of service. The contract should also state that the vendor is regularly audited for security purposes.
Termination: A contract must set forth what will become of the client’s data when the relationship is terminated. If possible, a provision should be included stating that the client’s data will be returned or destroyed within a predetermined amount of time.

As noted above, SaaS is a popular alternative to typical end user licenses that most businesses have grown accustomed to. With its cheaper up-front costs and focus on providing the most up-to-date versions, SaaS may be the perfect solution to a small company’s software needs. However, although the benefits of SaaS may be tempting, businesses must be cognizant of the potential problems associated with this model for obtaining software, and the dire consequences that may be faced in the event of a data breach or loss.

Kara Bufalino is an associate in the Firm’s corporate practice. For more information on SaaS agreements and related issues, you may contact Ms. Bufalino at 312/840-7050 or kbufalino@burkelaw.com.