

To SaaS or not to SaaS?

By John Simek and Sharon Nelson
© 2009 Sensei Enterprises, Inc.

Despite the often repeated *Jerry Maguire* line of “Show Me the Money,” implementing law firm technology isn’t always about the easily visible money. An even more important consideration is properly identifying the *real* cost of implementing a technology solution. We suggest that a traditional client/server model is generally the best solution for a law firm, not only from a cost perspective, but from control and security perspectives as well.

There is much marketing hype over SaaS (Software as a Service) offerings. Essentially, SaaS is a different way to spell ASP (Application Service Provider). Even *Wikipedia* confirms this renamed offering. To make it easy for readers to understand, imagine that you don’t own a copy of Microsoft Office – you simply go to a site on the Internet where you are, by subscription, allowed to use Office. The resulting data is held by the provider, not you.

The failure of the ASP model should still be fresh in many attorneys’ minds. Even as the stock market was bullish for technology companies, ASPs were busy flaming out. Clever minds on Madison Avenue therefore renamed the offering to get away from the stigma of the past and are making another run at it.

A name is not just a name. ASPs failed for a reason – and law firms would do well to remember the recent past. No matter what label you put on these products, law firms need to be very protective of their data and that of their clients.

The client/server model puts total control in the hands of the law firm. The data is held internally and access is controlled by the firm. You can choose to encrypt the data locally, which we recommend, or leave it in plain text. Either way, it is within the technology walls of the law firm and not directly accessible by any third party.

In contrast, the SaaS model puts your data in the hands of a third party. This is not necessarily a bad thing, but do you really know if the information is safe? Your contract with the provider may specify that the data be stored in encrypted form, but what if a disgruntled employee has access to tools that allow her to decrypt the data and sell your client data to the other side in a major litigation?

When you contract with a SaaS provider, you are required to accept the service as it delivers it to you. This means that any upgrades or bug fixes will be implemented by the provider. Sound like a good thing? Maybe so, but perhaps the upgrade requires you to pay additional fees or takes your old data through a conversion process that drops two very important field values, which have to be added back manually. The client/server model leaves the upgrade decision to you. You may elect to keep your current version since the upgrade doesn’t offer any significant functionality. This is a constant irritant for law firms as

very few are crazy about being forced into upgrades which cost money and/or require relearning some aspects of the software.

Besides the data security and access concerns for the SaaS model, the financial stability of the provider should be a major consideration, especially in these tough economic times. The last thing you need is to have the provider go out of business. Even if you have adequate notice, the cost to migrate your data to another provider or bring it back in-house can be significant. This brings us to the topic of exit strategy. At some point, you will likely want to bring the function back within your IT control or move to another provider. The contract should provide for specific costs and timetables to facilitate the move.

Another issue is the stability of the communications network. By design, you are dependent on the speed and quality of your Internet connection. Smart firms will have dual network connections to the Internet, although this will mean an increase in cost over what is normally installed at the firm. The Internet connection must be available at all times, otherwise you will not have access to your data. There aren't many judges that are sympathetic to your problems if you miss a filing date because your Internet connection went down. And Internet connections, as we've all miserably learned, do sometimes go down.

To be fair, let's look at the upsides of SaaS . . .

There can be some financial advantage to contracting service to a third party provider. Your investment in hardware and software is minimized since you are really only passing keyboard, mouse and screen data over the communications link. The actual processing occurs at the SaaS provider. All configuration and data hosting are external to your firm's infrastructure. Costs for the SaaS model can be based on the number of users or the amount of data storage volume. Either way, it is fairly easy to identify and budget for the cost of the service, which is a big selling point for a lot of firms. However, in order to get these "stable" price points, the contract terms are typically three to five years. This means that the firm must make a pretty long commitment to using the SaaS model and the specific provider.

Another advantage to the SaaS model is the rapid reaction time to changes. It is very fast to add new users or increase the amount of space for data storage. This is probably less of a selling point these days as more and more firms are in a contraction mode rather than expanding. Many firms like the mobility aspect of the SaaS model since they can access the applications from any machine with an Internet browser. Typically there isn't anything special that needs to be installed on the client computer. The user only needs a browser and perhaps a Java plug-in to access the SaaS application. This means that it is easy to gain access to the firm's data from the office, home or an Internet café in the Bahamas.

This easy access can also be a risk. Since the data is accessible from any computer, security must be very strong to make sure that only authorized personnel get to the confidential firm information. In a client/server model network, access can be restricted to allow only internal network access or specific IP addresses. This same restriction can be enforced by the SaaS provider, but you are still dependent upon the vendor to properly restrict access.

A good compromise to the traditional SaaS model is something we term a hybrid solution. The provider installs a rack unit on the firm's premises that contains all of the necessary hardware to provision a virtual environment. Just like a traditional SaaS implementation, the client computers do not do any actual application processing. Effectively, they are just dumb terminals that pass keyboard, mouse and screen data. The nice part about a hybrid solution is that the data is secured within the walls of your law firm. You are not dependent on the stability or bandwidth of your Internet connection. Normal processing occurs locally on your own LAN. It is inherently more secure since the information is not generally accessible from the outside world. The nice part about a hybrid solution is that you get the stability of having your data stored locally and lower costs because it is effectively a "drop in" solution. You can still remotely access the data and maintain greater control over the secure access.

Too often, all costs and all risks are not considered when analyzing a SaaS solution. The SaaS ballyhoo has drowned out all reasonable objections to SaaS. Clearly, we are not big fans, especially for law firm. Client/server solutions can be clearly defined from implementation through the life of the solution. You control the implementation, configuration and ongoing costs. While you can contractually specify some costs with SaaS, future upgrades and exit conversions may tip the financial decision.

Bottom line...keep control of your own data. It will be cheaper and less risky in the long run, even if the SaaS provider doesn't go out of business. And that nightmare scenario happened over and over again with ASPs. Historical lessons should not be undone by a change in name. Law firms are well advised to control their own data lest they find themselves explaining a data breach or inability to access data to clients, courts or disciplinary boards.

The authors are the President and Vice President of Sensei Enterprises, Inc. a computer forensics and legal technology firm located in Fairfax, Virginia. <http://www.senseient.com>