

Forewarned is Forearmed

For many companies, Software-as-a-Service looks an unbeatable proposition, but IT managers need to be careful about choosing their suppliers if serious legal risks are to be avoided, writes John Lang, IT Director of Epiq Systems.

Software-as-a-Service (SaaS) has become one of the true phenomena of the business computing market in recent years. Despite only existing as a concept since 1999, the global value of SaaS contracts is expected to reach \$10bn this year according to research consultancy IDC.

SaaS is used for a wide range of applications from email to personnel record keeping, customer relationship management software to computer-aided design packages. From the customer's point of view it reduces upfront costs, thus allowing maintenance to become someone else's problem. It also enables companies to use the latest versions of software without persistent upgrading expenses.

There has been a great deal of discussion about the pros and cons for companies thinking of using SaaS solutions, but relatively little about what the legal risks might be. Although the principle of SaaS is a sound one, using SaaS can create some real dangers for businesses if the right questions are not asked at the outset.

SaaS providers are able to provide a cost-effective service due to the economies of scale they achieve by hosting software remotely from their clients and effectively sharing it between a large number of different clients. In this situation, it is also common for the client's data to be stored on the supplier's servers. This is where the legal problems can begin.

Outsourcing the service doesn't mean outsourcing the risks. When it comes to data retention and security, the same issues that data managers have in-house apply when outsourcing to a SaaS provider. The task is more difficult because in a SaaS environment, IT managers no longer have day-to-day control over where and how their company's data is stored. Furthermore they have to rely on the supplier to ensure that standards are maintained.

The relative infancy of SaaS means that many of the potential risks have yet to be fully identified. Here, we outline some risks to be aware of and provide a list of questions you should be asking SaaS suppliers, preferably before entering into any sort of agreement.

What security is in place?

Data stored on a SaaS provider's servers will usually be encrypted, which is a good start. However, you need to be sure that the level of security will meet the data protection rules and regulatory requirements to which your company is subject. In particular, how is your data segregated from that of other users of the service? It is also important to know who within the organisation has access to the data, and where they are geographically located – if too many people are authorised to access and/or amend your data, it can represent a serious security and accountability risk. More generally, it is important to look into the background of the company providing the service, as well as the people that own and run the company. SaaS is a new industry, and if there are incompetents or rogues involved, it may be too early for this to have become evident without a high level of due diligence.

How is my data backed-up and how quickly can I recover my data?

Is your data stored in such a way that it can be quickly recovered in the event of litigation, regulatory, or criminal investigation? Is there a specific plan in place for the recovery of your data in the event of a regulatory request? The latter in particular can impose extremely tight timescales on companies to provide information and the failure to produce documents on time can reflect poorly. While, in litigation, the discovery process can take months, regulators often impose a 28-day deadline, yet it is not uncommon for the number of items involved in document reviews to run into the millions. A poorly-conceived back-up and storage system can make the e-discovery process extremely slow, which has, in itself, led to regulatory penalties being levied on companies when the response to an information request is too slow.

Deficient back-up systems can also lead to the loss of key documents, especially emails, and the failure to produce important pieces of evidence will almost always be viewed adversely by courts or regulators.

Checklist

- What is your company's data recovery plan? How long will it take to integrate the data?
- How will the data be backed up? Will this preserve the integrity, as well as, the substance of the data?
- Are you able to comply with my company's retention policy?
- Where will the data be stored?
- Who has access to the data?
- What is the background of the SaaS company and the people that will be looking after my data?
- What plans are in place to transfer my data should your company cease trading?



The author
John Lang, IT
Director, Epiq
Systems

Where is the data located?

Different countries have different data protection, security, and data retention rules. It is possible for companies to find themselves in breach of another country's rules, simply because its data is located on a server there.

In litigation, they may also find that information they thought was privileged (i.e. confidential) can be discovered by their opponents or by regulatory or fiscal investigators because it is on a server in a country with different data protection law. In some cases, it has even led to the courts or regulators of one country claiming jurisdiction over a case simply because a company's data was stored in that country.

So, when asking where your data may be stored, check whether there is a 'safe harbour' agreement in place that will insulate you against these problems and whether it will protect you in all circumstances.

Are you able to comply with my company's retention policy?

Many companies, especially larger ones that operate in regulated sectors, often have a myriad of data retention rules and regulations to comply with. If this is the case, it is essential to ascertain how much experience the SaaS provider has in dealing with multiple data retention policies. A key question to ask a potential SaaS provider is what experience does the Provider have in dealing with multi-national companies in your sector? It is also worth checking that their data retention and back-up extends to emails. Some regulators demand that these are kept for years, but are sometimes regarded as less important than other documents by some data storage and SaaS providers.

What strategies do you have in place to ensure business continuity?

The key question here is what happens in the event that the provider becomes insolvent and can no longer provide the service. Does the company have a robust contingency plan for

your data to be returned to you? If so, would the data be returned in a format which is easily transferable to another SaaS provider or back onto your internal systems? There is a lack of standardisation between SaaS systems, which can cause real difficulties for clients in this scenario.

Will the integrity of data be maintained?

It is not only the 'face value' of a company's documents that needs to be maintained in storage. One aspect of data management, that is sometimes overlooked, is the importance (and fragility) of the invisible 'metadata' contained in electronic documents. Much of the value of electronic evidence is often contained in its 'metadata', the invisible record of who has read a document, for example, or when it was amended.

This can be irrevocably damaged by the careless handling of electronic documents. In some instances, metadata can be destroyed or altered simply by copying files from one medium to another or just by turning a computer off and then on again. Failing to properly protect or produce electronic evidence, including metadata, can lead to negative inferences by regulators or the courts.

Hoping for the best – preparing for the worst

Getting any outsourcing contract right is always a matter of hoping for the best, but preparing for the worst. SaaS technology and services are so new that people aren't sure what is required under regulatory requirements. With SaaS, many of the potential problems are not immediately obvious and these issues often only get addressed when it's too late.

That is why it is important to ask questions about a provider's security policies and to review the credentials of the individuals administering those policies. It is critically important that companies get comprehensive answers before they jump into the SaaS environment. The cost savings are palpable, but the downsides can be significant if insufficient care is taken at the outset.