SRA Silver Linings:

Cloud Computing, Law Firms and Risk

In November 2013 the Solicitors Regulation Authority released a guide to Risk and Due Diligence for Law Firms looking to outsource their IT to Cloud Computing Systems.

We would echo the guidance of the SRA and strongly recommend that in order to reduce any levels of risk and to exercise proper due diligence, any firm looking at moving to a hosted system seeks these assurances from any potential supplier.

In providing the Osprey software package as a hosted system to our clients at the highest possible level we welcome this guidance and can of course confirm that we meet all of the requirements of the SRA.

The SRA Silver Linings guide to Cloud Computing states:

We seek to encourage the development of an efficient legal services market, and regulate based on risk. The Solicitors Regulation Authority recognises the benefits of advanced information technology architectures.

The SRA recognises that provided an effective provider is used, cloud computing can provide benefits for the firm and for clients, both in terms of costs and providing better levels of encryption and security.

1. Firms must be able to ensure that their provider can agree to SRA access to inspect data in order to meet Outcome 7.10 of the SRA Code of Conduct.

   Principle 7 of the SRA Handbook requires solicitors to comply with their legal and regulatory obligations and deal with their regulator in an open, timely and co-operative manner. Firms will in part be complying with the principle by achieving outcome 7.10 of the SRA Code of Conduct, the purpose of which is to ensure that they have appropriate terms in their contract of supply with the provider, allowing the SRA to access the information stored and visit the provider's premises where their data is held.

   All of our Client's data is held on our own datacentres, owned by us and based in the UK. Data held outside of the UK would of course cause logistical issue with a request for a site visit from the SRA. Our standard contract of service allows for site visits by the SRA whenever requested. We would also of course be more than happy to show you around one of our datacentres so that you may see the levels of security employed where your data will reside.

2. Use of cloud systems makes server downtime a business-critical issue. Firms must ensure that providers offer appropriate guarantees in regard to uptime and business continuity, and that data is protected in the event of technical failures or the provider becoming insolvent.

   We provide a 99.9% guarantee of uptime for the Osprey service. We operate multiple data centres that are mirrored in real time meaning that in the unlikely event of an issue at one datacentre (we operate redundancy on all constituent parts of the data centre and have fuel to run back up power generators for 48 hours!) another datacentre is also running in real time that is immediately available to guarantee the avoidance of any downtime whatsoever for users.

   Pracctice Ltd (the Company behind the Osprey Legal Cloud) has been running for over 26 years now and we have thousands of individual users paying for the service every single day. This regular, contracted income gives us a very sound financial flatbed to ensure that the company continues to run. Additionally, your data is of course always your data and we make available a facility for you to download a copy of this in an industry standard format (Microsoft SQL) whenever you wish. We also keep a copy of our software available in Escrow.

3. As part of basic due diligence, it is advisable to take up references, as well as asking for evidence of the provider's history of downtime and the steps they have taken to prevent future problems.

   In over 12 years of providing Osprey as a Cloud Based System, we have never experienced downtime that has caused outage across our mirrored facilities, meaning continuity at all times for our clients. Obviously, with any hardware, individual parts can fail but we ensure that each part (and each entire data centre) has a live working alternative provision to fail over to automatically to ensure the avoidance of any downtime for our clients.

   Having provided Osprey on a hosted basis for over 12 years we also have a wealth of firms that would be more than happy to provide a reference for the service and us as a company.

4. Use of cloud systems must comply with the terms of the Data Protection Act 1998. These terms require a written contract between user and provider and restrict the sending of data out of the European Economic Area ("EEA").

   Our Datacentres are based in the UK and no data leaves our datacentres. As we own these datacentres ourselves and do not subcontract to a third party for hosting your data we can guarantee that this will always be the case.

5. Under the Personal Information Online Code of Practice, if personal data is to be stored on a cloud, then there must be a written contract in place requiring the provider to act only on the user's instructions.

   This is provided for in our standard contract, firms that outsource hosting services to a third party may not be able to meet this requirement.

6. Given the nature of US surveillance laws, law firms should take into account how they use US-based providers or providers that use US servers. Firms should also consider the locations of the data centres and whether local laws could pose a risk to confidentiality by requiring the provider to disclose confidential information.

   We have invested heavily over the years building our own datacentres in the UK to offer this level of protection. With osprey your data would never leave the UK and we would not outsource the hosting of your data to a third party, whether a UK company or a US based company for these reasons.

7. Check that the provider can offer audited information security that at a minimum is compliant with ISO27001 2005

   Our Datacentres are ISO27001 compliant.

8. Outcome 4.1 requires solicitors to keep the affairs of clients confidential. This does not prevent firms outsourcing services. Indicative behaviour 4.3 is one way of evidencing compliance with the outcome, involving satisfaction that the provider has taken all appropriate steps to ensure that clients' confidential information will be protected. Firms should consider carefully the provider's systems for protecting confidentiality.

   Due to the economies of scale employed in providing a system for many thousands of individual users we can employ levels of both electronic and physical security to protect data way above and beyond the economic reach of any one individual firm.
   We fully comply with the Data Protection Act.

9. Providers often subcontract server capacity for reasons of flexibility, so may not be able to tell where any particular client's data is held

   This is only where providers have not invested properly in their own datacentre facilities. We would never subcontract any element of the hosting of our clients data to a third party.

   In outsourcing to a third party you would have a situation whereby your data would reside on a datacentre where other suppliers from other industries also have their applications hosted. This raises a concern in that the datacentre where your data resides is then accessed by an unknown quantity of engineers from companies unknown to you! As we would never outsource your data only our engineers have access to premises and equipment where your data resides allowing a much more secure environment.

10. To minimise the risk of being in breach of Principles 4 and 5, it is advisable to ensure that firms have the right to get data back in a usable format on demand and that they retain full ownership of the information stored. Firms should also ensure that they are aware of, and satisfied with, the arrangements under the agreement for: frequency of back up of data, continuity and portability of the data in the event that the provider's business fails (for instance through insolvency) or you wish to switch to another provider Escrow systems may in some circumstances be available to ensure continuity and control.

    Our standard contract confirms that the client is the owner of their data at all times and that we make available a facility for you to download a copy of your data in an industry standard format (Microsoft SQL) at any time you wish.

    By hosting our clients data mirrored in real time across multiple locations data is continually backed up to another live working site 24 hours, 7 days per week, 365 days per year.

    A copy of our Source Code is indeed held in Escrow for added peace of mind.

11. Given the importance of legal privilege and client confidentiality, law firms should exclusively use established, known and well-regarded cloud providers.

    We have been providing software to Law Firms for over 26 years now, over 12 of these have been on a Cloud Computing basis….before the term Cloud Computing was even used!

    We were the first Supplier to provide Cloud Computing to the UK Legal Market and believe that are still way ahead of other suppliers in the methodology of provision. We operate real time mirrored datacentres (not servers with an old fashioned dial up style connection!) that are owned by us (not outsourced to a third party!) and that are based in the UK.

For reasons of the guidance above we would always guarantee that your data would reside on multiple, real time mirrored data-centres, owned by us, not outsourced to a third party and based in the UK which we believe is a critical minimum requirement for any cloud computing provider.

The SRA Guide also highlighted the many advantages of a Cloud Computing System:

Cloud computing is continuing to increase in popularity, with low cost and flexibility the key advantages.

1. Cloud users do not have to maintain their own data storage or multiple site licenses for software. The cloud works out cheaper than direct data and program storage, and permits true mobile working with no need for data sticks or email transmission of files.
2. Sound cloud computing providers offer better encryption and security than would be possible for a small or medium-sized solicitors' practice storing its data locally.
3. It has been estimated that users of public cloud computing systems can see up front savings of 40-to-50 percent. Costs can also be flexible. Firms can pay for the software they use as they use it.
4. The same feature makes it simple for firms to upgrade their software and to introduce new types of machine, such as tablets for mobile working.
5. As processing power can be supplied centrally, users can obtain more advanced and effective systems that they would otherwise be able to run on their own network and machines. The economies of scale offered by large cloud providers also let them provide more potent systems at a lower cost, with a 5-to-10 percent efficiency saving on the pricing of systems.
6. The possibility of having software and data centralised on an accessible remote platform also allows for bring-your-own-technology policies, which some businesses have found to both motivate staff and reduce costs.
7. The fundamental point of cloud computing is that it does not matter what machine the user is working from. As long as they have their log-in details, then they should be able to access the same data and software wherever they are. This is an enabling technology for true mobile working, with fee earners able to access key documents anywhere. Even firms that do not intend to use mobile working, but which do need a certain amount of hot-desking, should see benefits from non-machine-specific access to data.

8. Cloud systems make it possible to have maintenance of IT systems conducted entirely remotely, by the provider. Maintaining local servers requires a local IT support staff, whether working for the firm or outsourced, to ensure that the systems remain operational. By contrast, with a cloud system, the servers are all the responsibility of the provider. This lack of any need to maintain an IT support department has explicitly been cited by one firm as a reason for adopting a cloud provision model.

9. The flexibility, cost and ease of maintenance offered by cloud computing systems make them simple for less experienced and well-funded firms to use. These systems may enable small law firms to gain the benefits of information systems that they could not otherwise access at all.

10. The use of cloud computing can improve general data security. Data service providers will usually have more experience in protecting data than their clients will, and have access to stronger security and encryption. The biggest data risk comes from lost or stolen laptops and USB drives. Google estimate that one in ten laptops go missing in the first year of use, and state that two thirds of workers report having lost a USB drive. Cloud systems remove the need for USB drives and mean that data need not be kept on individual laptops.

11. Use of cloud computing systems may also help in reducing the risk of data theft by employees. A 2009 survey suggested that one in three Wall Street and Canary Wharf workers had made unauthorised use of their employer's data. With audit trails and fewer untraceable means of storing confidential data, data theft is harder.

12. USB drives can also be a key vector for the transmission of Trojan Horse programs and viruses. Eliminating any need for them improves data security. Similarly, removing the need to transmit working files by email removes an insecure means of data transmission.

13. With data stored remotely on the cloud and with computers properly configured to require log-ins and passwords before connecting to the provider, information will not be leaked in the event of a burglary at the firm's offices

14. The intelligent use of cloud systems can reduce the risk of data or continuity loss. Most of the large cloud providers' service level agreements offer very high levels of uptime and the use of multiple backup servers and sites by such companies means that the risk of irrecoverable data loss is very low. Servers in a firm's own office, by contrast, can be lost in a fire or burglary.

15. Firms are increasingly using software as a service and cloud computing to deliver their IT needs. The reasons for this are price, flexibility and a desire for mobile working independent of specific machines. The high security and backup facilities made possible by the larger cloud providers are also desirable features.

16. Law firms whose use of cloud computing has been publicised have used it for purposes ranging from a cheaper and more flexible means of delivering traditional structures through to using it as an enabling technology for a fully virtual model.

You can view our website by visiting us here: http://ospreylegalcloud.co.uk/

A full version of the SRA Silver Linings guide to Cloud Computing systems can be found by visiting this website: http://www.sra.org.uk/solicitors/freedom-in-practice/OFR/risk/resources/cloud-computing-law-firms-risk.page