



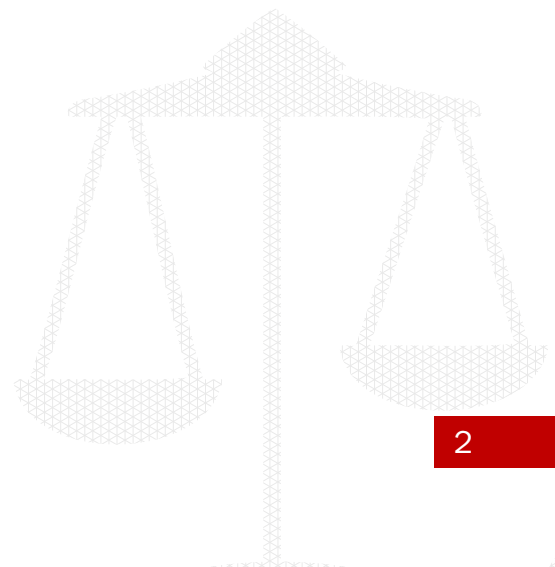
WHITE PAPERS

The Real Challenges and Benefits of Cloud Computing to Law Firms



Contents

Introduction	3
What type of cloud services are most suitable for law firms?	4
What does the SRA say about law firms using cloud based services?	6
What steps can a law firm take to increase the security of its data and protect client confidentiality in the cloud?	7
Can law firms safely use public cloud or must they only use private cloud?	9
What is the attitude of senior partners towards cloud computing?	10
Conclusions	12
Acknowledgements	13



“ Issues around data security remain as one of the biggest concerns about using the cloud.

”

Introduction

Simply put, cloud computing is access on demand via a network or the internet to services such as software functionality, computer processing and data storage. Due to the significant benefits cloud computing offers, namely flexibility, cost efficiency and scalability, it is fast becoming an attractive alternative to more traditional IT services. Alongside these benefits it also poses its own set of risks and challenges.

This white paper examines the opinions of a variety of law firms towards adopting cloud services. Furthermore it highlights the array of different cloud options and how different types of firms may take advantage of these.

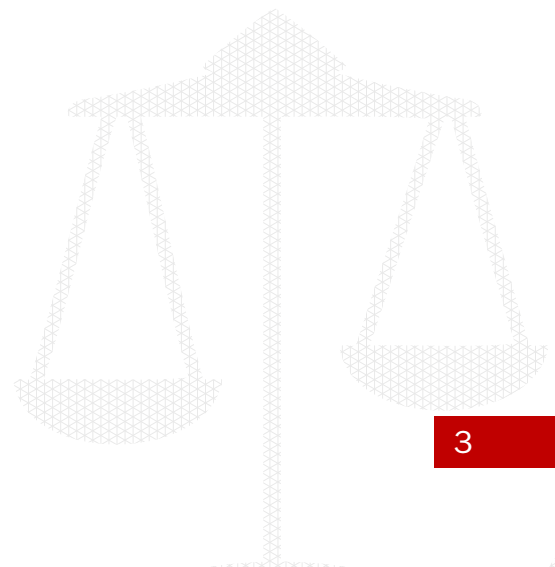
We interviewed a number of individuals, each holding a senior IT position within the legal sector. They told us under Chatham House rules about their views on the type of cloud services which are most suitable for law firms, the SRA's opinion and guidance on the use of cloud services and the steps a law firm can take to increase data security and protect client confidentiality when utilising cloud services.

Perhaps unsurprisingly our contributors provided a mixed response to a number of our questions but it is apparent that issues around data security remain as one of the biggest concerns about using the cloud. Lawyers are not alone on this – nearly every survey highlights the same key concern over cloud adoption. It is important to remember that cloud providers have heavily invested in increasing the security of their data centres and infrastructure and arguably they can provide a higher standard of security than an average law firm could ever hope to achieve.

Despite the perception of the legal profession as being cautious by nature and the real concerns around data security, a large number of law firms are already, and have been for some years, utilising some form of cloud services. Further, we are seeing a rise in the number of law firms adopting cloud services and this trend is set to continue.

Conversations with our contributors focussed on the key services of interest to, or adopted by, their firm and so this paper looks mainly at the use of Infrastructure as a Service (IaaS), Software as a Service (SaaS) and public and private cloud. It is worth noting that there is no generally accepted standard use of cloud terminology although NIST has adopted some definitions.

We were not surprised that our contributors used cloud terms flexibly and did not strictly adhere to the NIST definitions and therefore we have been equally flexible in our use of cloud terminology in this paper.



“...the take up of cloud-based services currently appears to be more prevalent among small to mid-tier firms.”

What type of cloud services are most suitable for law firms?

While the adoption of cloud-based services by law firms is on the rise there does not appear to be any general consensus that one type of cloud service is more or less suitable than another.

The contributors differed on what would be the best cloud service for a law firm as this will depend upon a number of factors.

“There is no simple ‘one size fits all’ solution for law firms - what is right for one firm may not work for another.”

What we can see is that the take up of cloud-based services currently appears to be more prevalent among small to mid-tier firms. Although theoretically all of the systems and applications used by a law firm can be moved to the cloud there are several factors a law firm will need to consider when deciding what type of service to adopt.

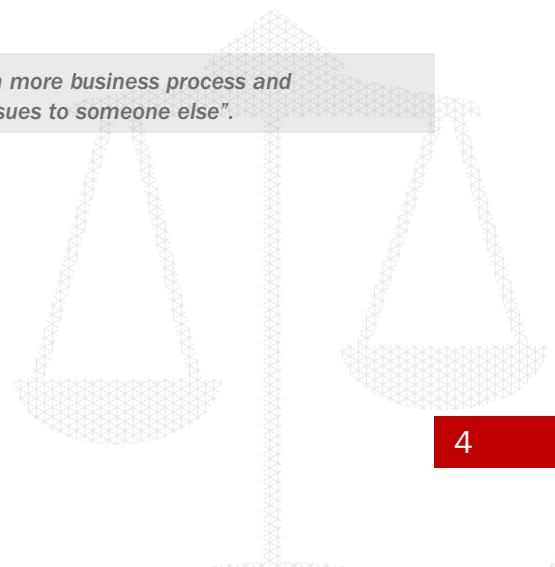
The contributors recognised that cloud computing is here to stay and that is difficult to try to prevent its adoption inside the firm but that the attitude of firm’s Chief Technology Officer (CTO) towards control of the IT systems is likely to be a crucial factor when determining the most suitable service. This contrasts with other businesses we have spoken to outside the legal sector who have adopted cloud – particularly SaaS solutions – without engaging their CTO.

“IaaS offers us greater flexibility and the firm can continue to utilise those software programs which are still under licence to it or bespoke systems developed by our IT team.”

On the whole our contributors indicated that Infrastructure-as-a-service (IaaS) could be better for larger firms which have made significant investments in their IT and have developed a number of customised key products. IaaS would allow the firm to keep everything largely as they developed it, thus retaining more control over its bespoke systems. One criticised IaaS as a “fragmented solution” due to the various service suppliers that the firm would require under it, and considered the ease of SaaS to be a more attractive solution. A further contributor said that, for the bigger more mature firms, the most suitable approach to cloud services is as a “points solution around the edges” but “nothing core should move to the cloud”. This recognises that the investment in an on-premise solution by larger firms could reduce the likelihood of a wholesale switch to IaaS or SaaS in the short term but allows them to acquire specific functionality through SaaS such as email archiving.

Conversely, smaller firms with smaller IT budgets might be less likely to have invested in the development of bespoke IT applications. This appears to give them a greater degree of flexibility to embrace SaaS more widely, thus freeing them up from having to maintain underlying infrastructure.

“SaaS allows the firm’s IT team to focus on more business process and strategic matters, leaving the technical issues to someone else”.



“ ...prior to adopting any cloud service the firm needs to carefully consider how their IT systems integrate. Failure to do this is likely to result in poor performance regardless of what service the firm adopts. ”

“ ...the argument for utility computing is powerful – firms can reduce costs, turn a fixed cost into a flexible one and grow their IT requirements in a flexible way. ”

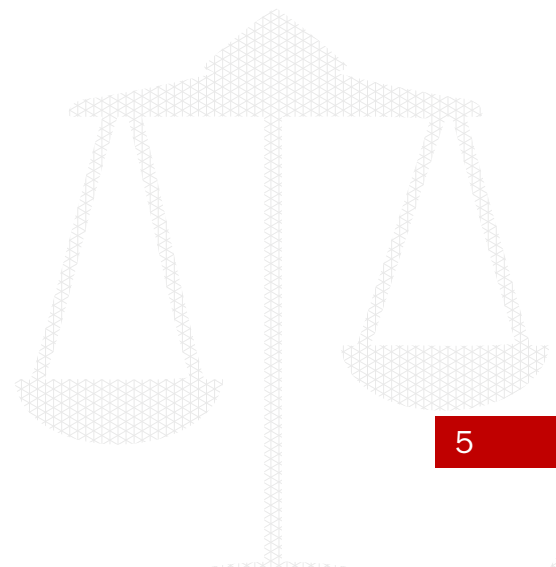
A firm's plans for future growth are another factor which can help determine the most suitable cloud service. Contributors noted a number of advantages of using SaaS for those firms looking to grow organically or through merger or looking to bring and keep their IT systems up-to-date. For example, because the service provider manages the software, SaaS allows a smoother, better controlled system for managing IT than trying to unify disparate systems in an IaaS solution. Also, since SaaS can be scaled on a per user basis, it is easier to grow quickly. Finally, as SaaS solutions are generally always on the same and latest version, SaaS can offer firms a faster method of upgrading, and an easier way to stay up-to-date. Another clear attraction of SaaS noted by one contributor was that it neatly created one port-of-call for all technical issues.

The interconnected systems of a law firm

Another contributor argued that moving a firm's IT infrastructure into the cloud is difficult and an “all or nothing” approach is required. The risk of carving up IT and only moving key parts of the infrastructure into the cloud could cause performance issues. In practical terms lawyers need to save documents on a document management system. This means that applications like Word, Outlook and the document management system ideally need to be located close together – it was felt that separating them could cause a decrease in performance at the desktop. A key message from this contributor was that prior to adopting any cloud service the firm needs to carefully consider how their IT systems integrate. Failure to do this is likely to result in poor performance regardless of what service the firm adopts.

A further influencing factor when considering the suitability of cloud services is undoubtedly cost. Cloud computing offers a pay-as-you-go approach avoiding high initial investment in hardware and software licensing and the ongoing maintenance and upgrade fees. As one contributor put it “the argument for utility computing is powerful – firms can reduce costs, turn a fixed cost into a flexible one and grow their IT requirements in a flexible way.”

One message we can take from our contributors is that it is still early days for law firm adoption of cloud services and at present while many firms are utilising some form of cloud services – SaaS in particular – there is still some way to go, particularly among the larger firms, before they fully embrace cloud computing. But as one contributor commented “Going forward there will be a time where the cloud infrastructure will mature and firms will start to question the rationale of running the IT systems itself. IT will become a utility.” This certainly tallies with the current view of cloud across all sectors.



“ Simply put, the SRA will not tell you how to get it right but they will tell you when you get it wrong. ”

What does the SRA say about law firms using cloud based services?

There is a distinct absence of any conclusive guidance from the SRA for law firms considering the adoption of cloud based services. As one contributor put it:

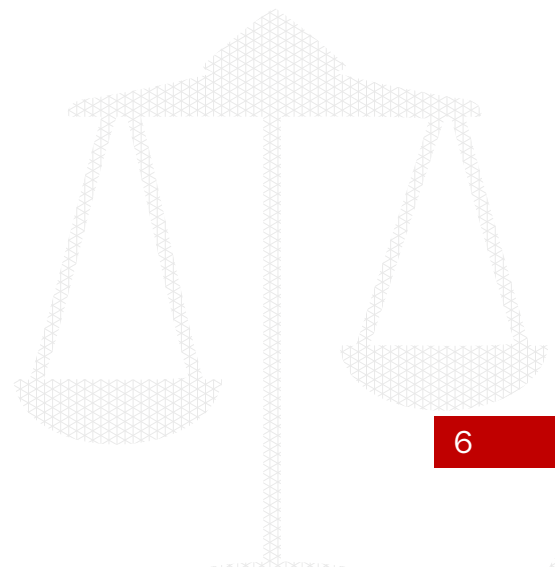
“It appears the SRA doesn’t have a view itself on this. Like everyone else, they appear to be in waiting mode. They’re waiting for something to go wrong.”

A common theme among our contributors is that the SRA’s primary concern is in relation to maintaining client confidentiality and data security. This is not surprising given that clients share sensitive information with law firms and it is widely known in the market that the solicitor-client relationship is protected by legal privilege. As a result, some of our contributors anticipated that the SRA may, in the future, become more involved in screening cloud services and ask law firms to provide detailed information on their cloud services. The SRA’s primary concerns are likely to centre around data storage; where is it stored, who controls access to it and what security measures are in place to protect the data from any unauthorised access.

Another contributor went further and said that, “law firms should ensure their contract with their cloud provider allows for the SRA to be able to obtain information from, inspect the records of, or enter the premises of the provider, in relation to the services provided to the law firm”. As the SRA has wide powers to investigate under the Solicitors Act it is important a law firm allows for this.

One contributor summed up the SRA’s position by saying “With outcomes-based regulation, the SRA is placing a responsibility on firms but without any backdrop. It’s a big ask of smaller, less tech savvy firms.” Simply put, the SRA will not tell you how to get it right but they will tell you when you get it wrong.

By contrast, the Law Society of Scotland has issued a fairly detailed advice note aimed to assist law firms determine whether cloud computing is right for them. This offers practical guidance as to how firms may minimise the risks associated with moving to a cloud based system. As well as addressing issues which should be included in an SLA the note stresses the importance of carrying out proper due diligence on the cloud provider, especially in relation to its data security compliance. Also, the Information Commissioner has published general guidance for organisations evaluating whether to adopt cloud.



What steps can a law firm take to increase the security of its data and protect client confidentiality in the cloud?

Surveys consistently show that the number one concern over cloud adoption is data security and this no different for our law firm contributors. The majority of our contributors identified data access controls and people as the weakest links in terms of keeping data secure. Again, this tallies with our findings outside the legal sector that data security is not just about the technology, but the people and processes too.

Even in the absence of definitive guidance from the SRA, there are several things a firm can do to increase security but as one contributor noted the starting point is to ensure the firm investigates before going ahead.

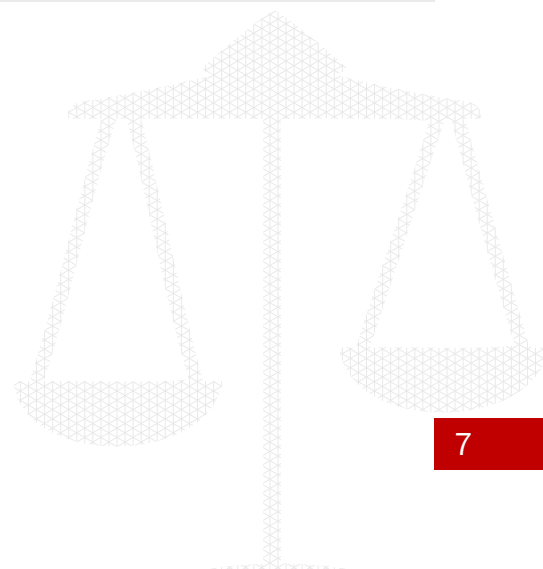
“As part of a firm’s due diligence it must ensure that it has the right controls over access to its data. For example, does the contract include the necessary confidentiality provisions and does the provider have adequate staff training and procedures in place?”

Also, firms need to ensure their staff are aware of the risks associated with different activities with one contributor pointing out that “people are more likely to obey rules if they understand them”. This matches discussions we have had outside the legal sector: if you educate the staff and, to some extent, empower them, they are more likely to comply.

All of our contributors commented on the fact that it is important to obtain assurances from the cloud provider that they are meeting industry standards by gaining appropriate certification. One contributor reported that his main priority was to ensure the appointed provider had achieved ISO 27001 accreditation for its data centre.

Another contributor felt it was important to use recognised cloud companies which enforce security and regularly undertake external penetration testing. This is an effective way to ensure your provider has adequate security measures in place to keep your data safe. He also said it is important to identify whether the data was stored on a public or private cloud. He commented that “if it is on a public cloud you have no idea where the data actually is. With private cloud you know where it is and you can lock down the information, create permissions and ensure greater security.” Of course, encrypting the data can strengthen security and this can be used in public and private cloud alike. Also, a cloud provider can provide a secure back-up of your data with a quicker recovery period.

“Cloud providers have greater knowledge, greater resources and the security of their systems constantly undergo penetration testing. No law firm can really compete with this.”



“ Our contributors’ general opinion is that leading service providers tend to have a firm grasp on security and arguably, offer levels of security far in excess of most internally hosted solutions. Data loss can, of course, occur whether your data is on-premise or in the cloud. ”

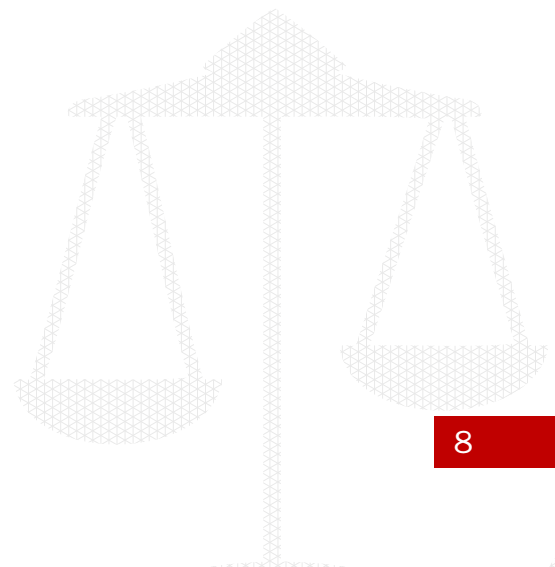
Interestingly, none of our contributors said they believe internally hosted data is inherently more secure than when stored in the cloud. This conflicts with those outside the legal sector we have spoken to who (incorrectly) hold the view that cloud is inherently insecure and on-premise is most secure. This either shows a greater understanding of the issues in law firms or a growing recognition of the real issues. Our contributors’ general opinion is that leading service providers tend to have a firm grasp on security and arguably, offer levels of security far in excess of most internally hosted solutions. Data loss - whether due to a hard drive crashing or someone hacking into your systems - can, of course, occur whether your data is on-premise or in the cloud.

Law firms must also have a plan in case their provider becomes insolvent to ensure their IT continues. If the provider outsources the storage of your data you will need to have the right to access that data. Including “step-in rights” in the contract could do this. Or, you could consider using a third party back-up or “data escrow” solution.

“You need to make sure you have a back-out plan. It’s not just the data you need you also need the resources to restore the whole IT system in a very short period of time. You need servers and network connections and you need them quickly.”

A couple of contributors explained that they have several possible strategies in place to cope with such a disaster, the preferred strategy being that the firm now maintains and updates local hardware as a backup that in an emergency they switch over to and can enable some or all fee earners to continue working as normal.

Essentially, when considering moving data to the cloud, a law firm needs to take a checklist approach and ask: what is the nature of the data being held in the cloud, who will have access to the data and how, in which jurisdiction will the data be stored, how will the data be securely transferred between the firm and the provider and does the firm have a plan if things goes wrong.



Can law firms safely use public cloud or must they only use private cloud?

Again, we received a mixed response to this question but the majority of our contributors appeared to favour the use of private cloud as being likely to reduce a firm's, a client's and arguably the SRA's concerns regarding confidentiality and data security.

One contributor said "private cloud offers better continuity with one provider supporting us and fully understanding our systems." The contributor emphasised the comfort provided from the fact that a private cloud is not influenced by external factors and there is no access or sharing to anyone outside of the network. Additionally, you require less IT and fewer staff on site as this can all be managed by the provider at its data centre.

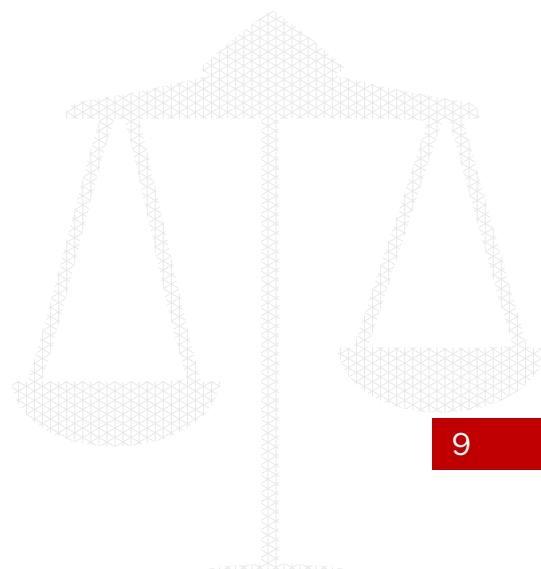
The contributors viewed the shared environment of a public cloud as a significant security risk with one reporting a nervousness around the inherent public nature of a public cloud. That is to say, it is a shared resource and as such it is a more accessible target to hackers and this is seen as posing a greater security risk. A public cloud solution is more likely to be accessed via the internet which was seen by some of our contributors as a vulnerability. But one contributor noted, "all forms of cloud are based on a shared infrastructure so the distinction between private and public seems false. Off premise private cloud may offer 'point to point' access but the data travels on the same fibre cables as the internet. Ultimately it is a question of risk and the vast majority of law firms, at this early stage of the development of cloud services are going to opt for private."

Even though private cloud seems to be seen as the safest and preferred option, security breaches are still possible. One contributor reiterated that people are the biggest security risk. The rise of our use of portable devices, including smartphones and tablets – the BYOD issue – increases our ability to access sensitive data. This offers employees and clients greater opportunities to send emails and other documents to their phones and other portable technology, resulting in potentially sensitive data now being stored externally in consumer cloud services. Law firms need to find ways to manage these sensitivities and minimise the risk of security breaches. These further highlight the importance of ensuring staff are properly trained and fully aware of the possible risks associated with the use of cloud based services.

Some contributors advocated a public and private cloud hybrid as the best approach. In this scenario the firm chose to store confidential client information in a private cloud, whilst using the more cost-efficient public cloud for HR and other less sensitive information. Another alternative put forward was the use of a virtual private cloud as "a possible middle ground which law firms may find to be an acceptable solution." This option provides a higher level of protection than that of a public cloud but the provider is still able to benefit from economies of scale which allows them to offer the law firm lower rates than that of a private cloud service.

“ ...people are the biggest security risk. The rise of our use of portable devices, including smartphones and tablets – the BYOD issue – increases our ability to access sensitive data.

”



Suffice to say, this is a fast moving area of technology and lessons are still being learnt. We know that data security is a key concern of a law firm when it is considering adopting cloud services. What our contributors are telling us is that a firm needs to think carefully about the nature of the data it holds and the various risks associated with a public or private cloud. A firm must carry out thorough due diligence before making any decisions, and as part of this, it is advisable to ask the cloud service provider to demonstrate their data security compliance and how they can protect the firm's sensitive data, whether it be stored in a public, private or hybrid cloud.

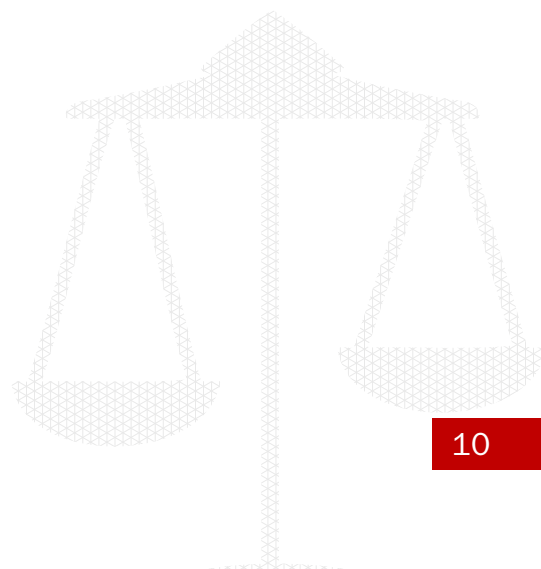
What is the attitude of senior partners towards cloud computing?

The attitude of senior partners towards cloud computing varies considerably. At one end contributors reported that the move to cloud based services was actually driven by senior partners, others felt that their senior partners were indifferent and not particularly interested while some said that significant persuasion was required to get the senior partners on side. Invariably the partners' attitudes will depend on the motivation behind the move – whether it be cost savings or because the firm is undergoing some sort of business transformation.

Interestingly, one of our contributors told us that what sometimes prevents a firm from adopting cloud based services is the resistance from its CTO. We were told that all too often the CTO has a lack of willingness to support the development of the firm and instead is worried about the security of his job and those of his team. Even so, partners seem reluctant to go behind the CTO's back and buy in SaaS resource. If this occurs the law firm is best placed to engage an external consultant with the necessary experience and expertise to put the different models on the table and present the case to the senior partners.

Another contributor explained that the main concern for his senior partners was the location of the data. There was an apparent nervousness about data possibly ending up outside of the UK and more specifically in the US or Canada. These concerns are twofold. First, the contributors are aware of the restrictions under the EU Data Protection Directive of moving data outside the EEA without proper safeguards. In fact, some contributors did not want their data moved outside the UK. Second, our contributors were aware of the potential access US government agencies may have to their data under the Patriot Act. This power extends anywhere in the world where the data is held by a US-owned cloud service provider. It was important to some partners that they could visit the data centre and physically see where it was stored and exactly who had access to it. This was easily overcome by selecting a UK-owned provider who stores all of the data locally.

“People generally gravitate to the path of least resistance, which is often the least secure path”.



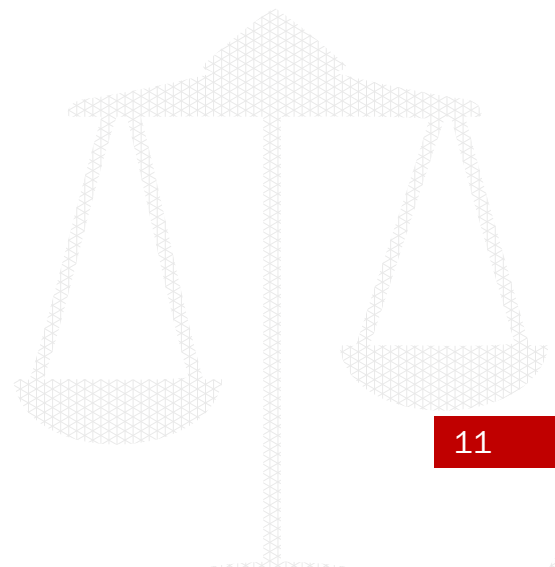
“ One contributor noted that the firm’s slow uptake of cloud computing was largely attributable to a lack of knowledge among the partners as to what cloud services are.

”

One contributor noted that the firm’s slow uptake of cloud computing was largely attributable to a lack of knowledge among the partners as to what cloud services are. Partners often use cloud services – in particular, consumer webmail accounts – in a personal capacity without even realising they are doing so. One contributor felt that the successful adoption of cloud services rests in the education of the relevant decision makers.

Unsurprisingly, reducing cost was reported to be one of the key driving forces behind a firm’s decision to adopt cloud based services. Notably, we only heard one contributor say that he did not see cloud as a cost saving model and this did not factor in his firm’s decision to move to the cloud.

Overall, the majority of our contributors told us that at the time they were considering moving their IT infrastructure to the cloud the firm had reached a point where it needed to make significant updates and changes to its IT system. This appears to cultivate willingness among partners to a move to the cloud. As we mentioned earlier, firms are most likely to consider moving to the cloud when they are faced with major technology upgrades or some sort of business transformation. Consistent with all of the firms we spoke to was that the two most important factors in the senior partner’s decision is reducing cost and assurances that the firm’s data would be stored within the UK.

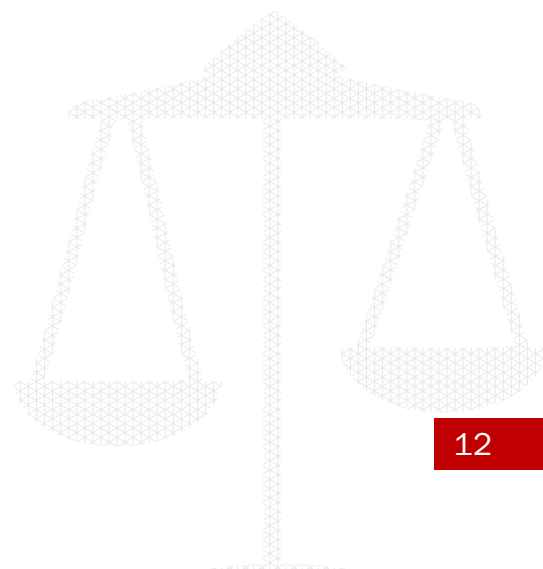


Conclusions

From the discussions we held with our contributors and from our own experience, we reached the following conclusions.

1. The legal sector seems to be embracing the adoption of cloud albeit in varying degrees although, at least for now, the SRA is not providing any definitive advice.
2. It is clear from listening to the contributors that when deciding whether to adopt SaaS, IaaS, private, public, hybrid cloud or other there is no right or wrong answer - indeed, there are some disparities over use of these terms. Instead, each law firm will need to consider a number of factors before deciding what solution is most suitable. First and foremost law firms must have a clear plan on what the current and future IT needs of their business are.
3. We have seen that the smaller to mid-tier firms or those looking to grow quickly may be more likely to adopt SaaS, whereas the bigger more mature firms, operating more bespoke systems might be better suited to IaaS. There are certain discreet functions such as, email spam filtering and secure file transfer solutions which appear to be ideal candidates for SaaS adoption.
4. Due to the sensitive nature of data that a law firm holds, it is imperative to acknowledge and address data security and protect client confidentiality. There are concerns over using public cloud although this is not necessarily based on proof. Furthermore, partners do not automatically correlate their concerns over public cloud with their use of personal webmail accounts.
5. A firm can take steps to protect itself in the cloud by carrying out proper due diligence on any proposed provider, ensuring the provider has obtained appropriate security credentials and by seeking to negotiate proper safeguards in the contract. A firm also needs to monitor and control use of unauthorised cloud services by the staff.
6. Additionally, it is important when adopting a new cloud system that there is a sufficient disaster recovery plan. Although law firms generally accept that cloud providers have better resiliency than an individual firm may have, things can still go wrong. A sufficient disaster recovery plan is therefore necessary to reduce recovery time and make sure there is always a back up of the firm's data.

On the whole, there is strong awareness of cloud in law firms and widespread acceptance that appropriate adoption of cloud solutions in law firms can benefit the firm.



Acknowledgements

Our thanks go to those senior executives who gave their time so generously to contribute to this study, either through interviews or telephone conversations.



Berwin Leighton Paisner
www.blplaw.com

BLP's international lawyers apply fresh thinking, legal and market experience to provide clear legal advice aligned to the commercial objectives of our clients. BLP's clients rely on our expertise to find straightforward, actionable legal solutions that help them to take advantage of opportunities, tackle problems and defend their rights.



DMH Stallard LLP
www.dmhstallard.com

DMH Stallard is different from the law firms you might be used to. To put it simply our clients enjoy a business-like approach to project delivery and partner led legal advice that is amongst the best in the country.

We invest time in our client relationships so that we always provide exceptional levels of service. Our clients like our approach and we now work with some of the most successful organisations in the country.



Sidley Austin LLP
www.sidley.com

Sidley is a global law firm committed to providing excellent client service, fostering a culture of cooperation and mutual respect, and creating opportunities for lawyers of all backgrounds. With more than 1,700 lawyers in 19 offices around the world, talent and teamwork are central to Sidley's successful results for clients in all types of legal matters, from complex transactions to "bet the company" litigation to cutting-edge regulatory issues.



Stephens Scown
www.stephens-scown.co.uk

You can turn to Stephens Scown for help in your business, financial or family life. Sometimes it might be with an opportunity, sometimes a problem. Either way, you know you're guaranteed friendly, honest and professional help from a team of legal experts who always have your best interests at heart.

It's a refreshing approach to law which has seen us forge long-lasting client relationships, some stretching back more than fifty years.

The Real Challenges and Benefits
of Cloud Computing to Law Firms

www.databarracks.com



Thomson Snell & Passmore

Thomson Snell & Passmore
www.ts-p.co.uk

Thomson Snell & Passmore is a law firm with a reputation for providing high quality, intelligent advice. Our approach is always practical, realistic and commercially based.



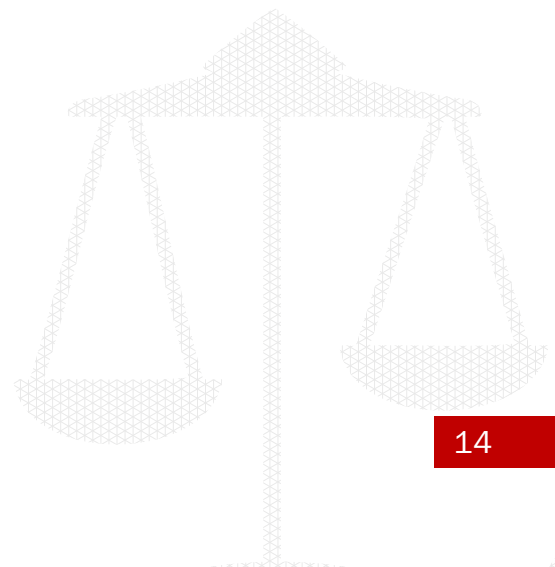
Change Harbour
www.changeharbour.com

Established in 2011 Change Harbour delivers high quality, innovative technology solutions to the legal and broader professional services sector. Change Harbour combines over eighty years experience working in and leading some of the highest profile professional services firms in the world. We exploit this experience to deliver solutions and services that help our clients achieve their strategic goals and maximise the benefit from their investments. One of our key objectives is to bring great technology to the professional services sector that has been proven and successful in other sectors. We offer a variety of software solutions and implementation services in a number of areas including information and content management, news aggregation and distribution, mobility and business analytics.



Large International Law Firm

A large International law firm with offices in over 30 countries. The firm provides clients with a broad range of business advise in a number of practice areas including banking and finance, real estate, as well as, litigation, intellectual property and commercial dealings.



The Real Challenges and Benefits
of Cloud Computing to Law Firms

www.databarracks.com



About DMH Stallard

Frank Jennings

Commercial and Cloud lawyer at DMH Stallard LLP and Chair of Cloud Industry Forum Code of Practice Board

Frank is a lawyer specialising in cloud & technology, data security, intellectual property and commercial contracts. Frank chairs the Cloud Industry Forum's code governance board and co-authored CIF's best practice recommendations in Cloud Contracts. Frank guides clients in drafting cloud contracts and ensuring data security compliance. Independent legal directory Legal 500 rates him #1 for Technology.

Frank blogs at businessbeanstalk.net and regularly presents on cloud and data security issues.

Contact Frank for more information on how to keep your data secure in the cloud and how to de-risk your cloud contracts.

frank.jennings@dmhstallard.com

DMH Stallard is proud to work with some of the most innovative and successful organisations in the country, including major financial institutions, FTSE listed companies, private equity backed businesses and high profile public sector bodies. We are also delighted that the firm continues to be recognised with industry awards and in 2012 was awarded the Corporate Law Firm of the Year at the prestigious Insider Dealmakers Awards.

businessbeanstalk.net

www.dmhstallard.com



Databarracks provides secure, Infrastructure as a Service, Backup as a Service and Disaster Recovery as a Service from UK-based, ex-military data centres.

Databarracks is certified by the Cloud Industry Forum, ISO 27001 certified for Information Security and has been selected as a provider to the G-Cloud framework.

www.databarracks.com

Phone: 0800 033 66 33

Email: info@databarracks.com

