Cloud computing is the name given to the delivery of a range of services via the internet, instead of via bespoke infrastructure or software. In effect, it is remote computing services - that enable a business to access data and software in the ‘ether’.

The benefits of the cloud include increased efficiency and remote access to your company’s computer system. This makes it particularly practical for companies with geographically dispersed or mobile workforces. Cost is another significant advantage alongside adaptability. With both large and small businesses looking to streamline IT infrastructure, cut costs and remain as flexible as possible, cloud technology can be an attractive proposition.

Unsurprisingly, sales of cloud services are reportedly rising by 24% annually, according to International Data Corp figures. The United States leads the market in cloud services, and it is estimated that the market in Europe is approximately two years behind in terms of acceptance and growth. However, with the developments in mobile technology and the economic crisis continuing in Europe, interest in the cloud from European companies is rapidly increasing, and the indications are that cloud services will become as popular in Europe as they are in the US within the next couple of years.

On the flip-side, however, the risks are significant. Companies are handing over the control of IT systems and data to a third party supplier. But as the data owner, companies retain responsibility for the data.

Questions that organisations need to ask are:

- Where is our data being held?
- How secure is the data?
- What happens if the cloud supplier’s server goes down (as happened to Amazon’s cloud service in early July, due to a lightening strike at is technology centre)?
The main risks of the cloud

Data security – with cyber criminals getting increasingly daring and sophisticated, data protection and security is vital. Regulators in the US and Europe are tightening laws around remote data storage requirements. In Europe new guidelines due for publication are designed to make cloud services in Europe more secure, but potentially more expensive. Providers will be required to inform clients as to where their data is being stored, and give details of all subcontractors that they use to process data. For data transfers between Europe and the US, the guidelines recommend that clients demand that their data is being protected in line with EU law in terms of reporting and auditing.

System failure – as a number of companies including Netflix discovered, when Amazon’s cloud service failed, connection downtime can pose a major problem if it cuts users off mid-business transaction, or whilst a remote diagnosis is taking place. You need to consider what would be the impact on your sales and brand reputation if such an outage occurred for a prolonged period? If the system fails what happens to your data and what recourse do you have? Does the cloud provider have adequate disaster recovery plans to restore its service and in what timescale?

Longevity – what happens to user data if your cloud service provider goes bust or is acquired by another company? Before signing up with a provider we recommend that clients undertake due diligence checks, and understand what systems are in place for data retrieval, and in what format the data will be supplied in. If you wish to end your contract with a cloud provider, what will happen to your data? Will it be deleted, and if yes, will this be done securely? These are elements that should be covered within your contract.

Data location – a cloud provider will not necessarily know in which jurisdiction a user data is stored in. This can create problems linked to local privacy requirements as the laws vary from country to country and this is a legal issue being considered by governments around the world – especially with communications being increasingly mobile.

Data segregation – as data is kept in a shared environment alongside other customer data, there can be issues relating to data encryption. Can you ensure your data is kept segregated and ring-fenced?

Illegal activity – cloud services are hard to investigate as they are often spread across an ever-changing set of hosts and data centres. Users should get contractual commitment to support specific forms of investigation.

Managing the risks

If you are contemplating using a cloud provider you need to consider the risks to your business and its brand, should a data breach occur, and then put a cloud specific risk management strategy in place. You need to understand what service level agreements are in place, as these should help to address the risks associated with your data while it resides in the cloud. You need to consider where your data is stored, how it is protected, how and when you will be told if a data breach occurs. A business needs to be absolutely clear as to where responsibility for security and compliance to the SLA falls.

Before signing any contracts with a cloud service provider we advise that your legal advisers go through the contract, and they identify your company’s liability exposure. Many cloud service providers offer little or no indemnity against the majority of liabilities associated with data loss or a data breach from their system. We advise that a vendor risk management programme is put in place, that will help you to monitor your relationship with your cloud provider, and help you to minimise the risks.

There is also a growing insurance market for both first and third party data liability business, as well as first party business interruption cover. These products and covers are likely to continue to develop over the coming years. However, this is still a very specialist market and so it is advisable to use a broker which specialises in data risk.

For more advice on managing risks associated with using a cloud service provider, or to find out more about insurance solutions, please contact us.