Cloud security - exploring the risks

By David Stubley, CEO, 7 Elements

As an information security professional, I am often asked about the Cloud, in particular **"Is the Cloud safe?"** and **"Should I use the Cloud?"**

For me the starting point should be: **"What data do I want to put in to the Cloud and how important is that data to me in terms of confidentiality, availability and integrity?"**

The answers to these questions, combined with an appreciation of the risks associated with using the Cloud, will then enable you to decide if using the Cloud is the best option for you. More importantly, it will allow you to manage the risks involved. This approach will enable your business to meet its objectives whilst managing the risk to an acceptable level.

Cloud basics

What is the Cloud? Well, in short, it is a great marketing buzzword. There is no one individual such thing as the 'Cloud'. The Cloud is a term used to describe multiple service offerings such as Software as a Service (SaaS), Platform as a Service (PaaS) as well as Infrastructure as a Service (IaaS). All these are characterised by the use of on-demand provision, rapid ability to scale and are based on payment solely for the amount of resource required at any given point. Cloud provision often makes use of shared virtual services for the storage and processing of data.

Organisations can implement their own 'Cloud' or can partner with an external supplier to use their external party's infrastructure. The basic premise is that you only provision the services required to meet your needs and that you can then grow and shrink this as required, with the organisation only paying for the resource consumed.

Key Risks

What are the key risks presented by using the Cloud? For me, the key risks and some of the issues that an organisation should explore are discussed on the next page.

What legal jurisdiction will my data be held within?

As an organisation you should be aware of how legal requirements to disclose data may be affected by the geography of where the data is stored. If you are based in the UK and use a US based Cloud provider, consider the impact on your organisation if the US courts enforce disclosure of your sensitive data. Where the Cloud is used to store or process sensitive personal data, there may be an impact on your compliance with the required regulation (Data Protection Act,) which you will need to fully understand and mitigate.

Will your Cloud provider place your data in multiple geographies without your knowledge?

Different geographical locations mean different legal jurisdictions, which will have an impact on your legal and regulatory requirements within each of those regions. This may restrict the type of data that can be stored or processed or limit how the data in question can be transferred between locations. The ability to encrypt data will also be impacted within certain locations due to export restrictions.

Who else may have access to my data?

Many Cloud services are based on the use of shared services or multi-tenancy solutions. The benefit to the end user is reduced costs, but this can also lead to security concerns. The data may be at risk of attack from another user of the same Cloud service due to the architecture in use. Consideration should be given to how the Cloud provider has limited the possibility of data compromise.

Will my data be destroyed securely?

As discussed earlier, the idea of the Cloud is that you can grow and shrink your resource requirement. When the data on disks is no longer needed then it will need to be destroyed. You will need to gain assurance that this has been destroyed in compliance with your organisation's standards, that the next user of that environment will not accidentally gain access to your data, and that you have met any regulatory requirements.

What other unintended consequences need to be considered?

The list above is not exhaustive and there will be other issues specific to your organisation that will need to be explored to enable you to make an informed decision about using the Cloud. There will also be further unintended consequences that the Cloud will introduce and as many of these as possible should be identified to enable a robust risk managed approach to be undertaken.

Bringing it all together

The Cloud offers a cost effective and flexible approach to manage your data storage and processing requirements. However, the Cloud is no different to the wider challenges of managing an organisation's data securely. With these unique opportunities, unique risks will arise. A sound understanding of these risks will enable an organisation to assess if the Cloud is right for them and if it sits within the overall organisational risk appetite for data security. Risk areas identified can then be used to structure any assessment of potential providers to ensure that they can meet your requirements and that the contract will legally enforce this.

7Elements
Independent information security consultancy

7 Elements Ltd,
West Philpstoun Steading,
Old Philpstoun, Linlithgow
EH49 7RY

T: 01506 830 829
www.7elements.co.uk