ANDERSON
IT MANAGEMENT

Cloud Computing

Enabling a flexible and productive workforce, with secure access to company data

Cloud Computing has provided businesses to remain agile and competitive in today's market, but how do you know what "Cloud" to choose?

"The Cloud" can be daunting to business owners, as there if often a lack of understanding in how the technology works and if your data will remain private and secure. It is therefore important to ensure when choosing a Cloud Computing platform that you have a clear understanding of the benefits to your business (number one tends to be cost savings), the risks (will my data be secure?) and the ease of use (do I need to re-train staff?).

01 How do you use your computer today?

For the majority of businesses, the personal computer provides you with the ability to communicate and conduct business with your customers by using common or bespoke applications all with access to your company data. The key to agility and productivity is access to that data.

02 How does Cloud Computing help?

Cloud Computing removes the isolation of company data and applications being stored on an office-based fileserver by providing "rented computing space" on a hosting company's server that can be accessed from any device (personal computer, tablet or smart phone) via the internet.

Cloud Computing is simply using a 3rd party provider's server (or servers) to store your data. Great examples of these types of companies include Microsoft, Amazon AWS, Google, Apple and DropBox.

Benefits of Cloud Computing are that it:

- Removes the need for workers to be in the office to access IT systems
- Enables a flexible and remote workforce
- Improves security and reduces management cost of maintaining your own company server

03 Is my data safe?

Your data should always remain your responsibility. Robust and reliable processes for protecting and recovering your data should always remain paramount for any computer system, whether this be private inhouse systems or hosted on a 3rd party's Cloud Computing platform.

Your data will always be safe if you retain control of the protection of the data.

04 How do I choose the right Cloud Computing platform?

There are 3 main distinctions for Cloud Computing technology:

- Public Cloud
- Private Cloud
- Hybrid (combining both of the above)

Public Clouds are provided to the worldwide audience and host thousands of businesses and consumer users. Public Cloud providers include Microsoft (Office365 and Azure), Amazon (AWS), Google (Mail, Docs and Applications) and DropBox (shared file storage).

Public Clouds come with a higher level of risk based on the number of users they host, and do not provide you (the customer) with any control of the computing infrastructure.

However, Public Clouds offer the best level of agility and can scale very quickly to meet new demands if you need more storage or more computing power. They can also shrink in size, enabling your business to control costs and only pay for what you consume.

Private Clouds are dedicated servers for your business only and are not shared. They can be located securely by a 3rd party hosting provider but they allow you to retain full control of the servers and data.

Hybrid combines the two cloud solutions together. Where a Private Cloud system can extend its resources into a Public Cloud provider for controlled periods of time such as when workloads demand extra power for certain periods, or if the long-term storage of data (e.g. archive) can be stored for a lower cost.

ANDERSON
IT MANAGEMENT

05 **My servers and data are now accessible as a "Cloud Service" but how do I control the end user's computer?**
The End Point or End User as they are described, remains to be the most important area to secure. The end user's computer tends to be the costliest to maintain and is the most common point where threats occur or malware is injected.

Cloud Computing Online
If your business can adopt to running systems online (ie. everything you do is in a browser or on a website page) then your end user computer requires much less "local" support and protection. The great example here is the Google Chromebook, which only runs a Google Browser application.

Online Computing offers many advantages, including automatic saving and versioning of documents, and collaboration of data where one document can be worked on by multiple people, at the same time.

However, not all businesses are able to adapt or can make full use of Online Applications, and therefore require the end user to have more capable computing device (e.g. a Windows Desktop) that provides both local computing power as well as online access to Cloud services.

The Full Desktop requires the most security as it can store data outside of the Cloud Computing infrastructure. This may be a requirement for some businesses who work with larger graphics files or need access to data offline. Full desktops therefore require security software and backup processes to protect it.

06 **The Virtual Desktop**
To enable a highly secure Private Cloud computer system, businesses are considering a Virtual Desktop Infrastructure (or VDI). This provides the end user access with a fully functional desktop from any device (e.g. their own home computer) while maintaining the security of data within the Cloud computing platform.

What else do I need to consider?

There are some additional key things to consider that should form part of your overall strategy as you make the journey towards Cloud Computing.

01 **Access, Secure Passwords and Multi-Factor Authentication**
Ensure you have a strong set of policies relating to security and access to IT systems, which should be the same policy if you choose Public or Private Cloud solutions. Minimum requirements should include:

- 10-15 Character Passwords (3 random words, upper and lower case and special characters)
- Multi-Factor Authentication (a 2-step process to gain access to your systems)

02 **Cyber Training for your team**
Cloud Computing does not keep you safe from Cyber Threats. Regular Cyber awareness training should form part of your company handbook and people processes. This makes your users aware and knowledgeable on the topics of ransomware, phishing emails and how to safely share data.

03 **Data Encryption**
Data should be encrypted, on the Cloud Servers (while at rest) and in transit when sharing with colleagues, customers, or suppliers.

Public Cloud platforms have this facility but not always as a default setting. Private Cloud platforms will require additional encryption software to be added.

End User computers running Windows 10 or Mac OS do not turn on encryption as standard, but the software is ready for encryption to be enabled.

PDSC
POLICE DIGITAL SECURITY CENTRE

For more information
website: www.andersonitmanagement.co.uk
enquiries: 0115 871 6516
email: info@andersonitmanagement.co.uk