

Data security critical for cloud-based solutions

By [Stephen Garbett](#)

9 Apr 2019

Traditionally, data used to be a physical asset that required on-site protection. However, in the digital age, data can be located anywhere in the world thanks to the adoption of cloud solutions. Of course, this does not mean its security should be any less of a priority as data has become the lifeblood of an organisation.



Stephen Garbett

This requires a different mindset as security today is as much the responsibility of the cloud service provider as it is of the business using it. In the past, many businesses struggled with keeping their cybersecurity measures up to date, making them easy targets for hackers and malware to compromise their systems.

In a cloud environment, security is one of the foundational priorities. Service providers need to meet stringent Service Level Agreements and build their offerings on their reputation to safeguard data whether threats come from hackers or elsewhere, such as natural disasters. After all, if a business stores its data in the cloud, it has the added peace of mind that redundancy is on hand if, for example, the office should burn down.

And yet, it has still taken time for decision-makers to trust the cloud as a safe and reliable place to store organisational data.

Legislatively-driven

The General Data Protection Regulation of the European Union is driving the impetus to view data, and its storage requirements, differently. Regulatory requirements today are focused on ensuring the integrity and security of data on an individual level.

Thanks to the pervasiveness of mobile, people are connecting to systems in different ways and accessing information irrespective of location, time, or even device used. Furthermore, the growth of the Internet of Things is seeing information being recorded in different ways and used for a variety of things from customised marketing to identifying sales trends.

Numerous local and international data breaches have made people increasingly aware of the implications of not keeping their personal information safe. And from a data security point of view, companies understand they must get their houses in order to ensure they do not fall foul of legislation.

Adoption rates

Increasingly, multinational providers are rolling out data centres in new territories throughout the world. More recently, South Africa saw the introduction of two Azure data centres that will likely speed up adoption and growth of cloud technologies across business sectors irrespective of company size in that country.

However, the increasing global adoption rates of cloud services will put even more pressure on businesses around the security aspects of data. For example, in the UK things like cost-savings and availability of data are underpinned by security measures and how best to balance all the requirements for a digital age.

And yet, despite technology innovations around the cloud, there will not be that much of a shift happening around the cyber security focus of it all. Instead, service providers and businesses will likely cement practices that have been put in place. It is all about tying up loose ends and ensuring all entries into the business are protected.

So, from a technological level, not much is expected to evolve but businesses will certainly grow in their adoption and how they use the cloud for their data storage and analysis requirements.

ABOUT THE AUTHOR

Stephen Garbett, MD of Decision Inc. UK

For more, visit: <https://www.bizcommunity.com>