BY
Jason McLaughlin

Jason McLaughlin, Trusted Adviser, Ortus, Managed IT & Cloud

Security & Cloud Computing

Jason McLaughlin looks at some of the misconceptions concerning Cloud Computing and Data Security and what the real security risks are.

Data Security is a concerning factor when using any level of Cloud computing and rightfully so, however there are some misconceptions regarding security threats as well. In this article we will try to filter through the unfounded concerns to help reduce misperceptions so that more focus can be placed on addressing cloud security threats that should be prioritised, ones that are real, rather than fretting over fictitious issues.

Cloud Computing has become a more mature technology and now a way of computing that many are familiar with and even confident with using on a day to day basis. Nevertheless, confusion surrounding cloud security hinders the comprehensive adoption of cloud. By no means should we become complacent towards security in the cloud but we should be knowledgeable enough to understand and differentiate fact from fiction, to make informed cloud decisions based on true concerns rather than on concerns that are no more than mere myth.

Hopefully through clarifying the real security risks and disregarding the misperceptions, the route to a more comprehensive cloud may become clearer, security can be more effectively managed and provider choice made simpler to attain.

Data security, not as secure in the cloud compared with secured on premises?

Some companies question the level of security offered by a cloud vendor. They often incorrectly consider their data to be more secure on their premises behind their own firewalls. However, this is not always the case.

Cloud vendors put all their efforts and resources into ensuring that their data centres are as secure as can be. They conform to strict compliance standards and access to data is strictly controlled. Whereas on premise access to company data from within the company is often very relaxed with servers holding critical data usually not secured. Access to the data is easily achievable by employees hence easily breached, often the result of an inside attack.

Cloud vendors offer numerous data centres, backup, disaster recovery and layers of security. These are frequently audited to keep security up to date.

The truth is that data is likely to be more secure with a reputable cloud vendor than on most businesses own premises. It's becoming exceedingly difficult for businesses to stay on top of security, patches, upgrades and vulnerabilities with the same tenacity and dedication of a reputable cloud vendor.

Public Cloud and Security

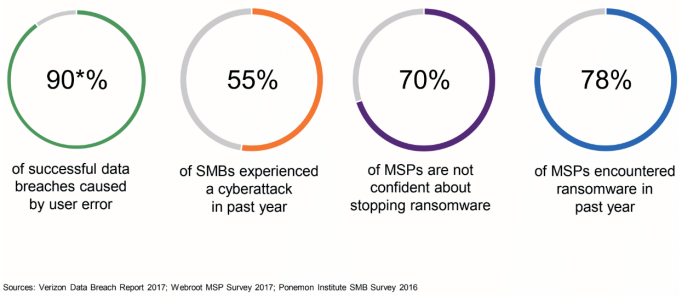
A common misconception is that if you have your data in and are serviced by a public cloud, others using that cloud can access your data and you will also be more vulnerable to attack from others utilising the same public cloud.

This is not correct. You are sharing the cloud resources with others but you are secure within the multitenant environment if the proper measures to segregate data are in place. Precautionary security measures such as encryption and access control need to be in place to ensure that a breach is not likely to occur.

It comes down to due diligence and making sure the provider you choose has the necessary measures and policies in place to satisfy your security needs.

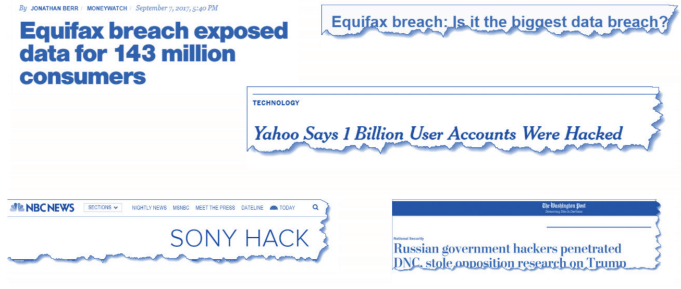
BY
Jason McLaughlin

The High Cost of User Error



Sources: Verizon Data Breach Report 2017; Webroot MSP Survey 2017; Ponemon Institute SMB Survey 2016

Cyberattacks are making headlines!



Applications in the cloud

There is a misconception that traditional PC or server software undergoes superior vetting compared with that of cloud applications, making traditional software more secure and reliable.
This is not the case.

Cloud applications are continuously monitored, maintained, patched and kept up to date, whereas PC or server software updates are wholly reliable on the end-user doing this. Within a business the likelihood of this being undertaken daily or even weekly is slim but this is commonplace within a cloud environment of a reputable cloud provider.

Outside threats, breaches and the Cloud

Many consider the cloud to be more vulnerable to outside threats than a typical onsite IT environment. This is not true. All environments need to be secured adequately to secure against any potential threats. Firewalls, vulnerability scanning, network security technologies and encryption should be used. This is not unique to cloud environments but necessary for all environments. If the cloud is properly secured it does not have to be more vulnerable to outside threats or pose any heightened security risk.

All clouds are created equal?

The cloud is not generic and all clouds are not the same. Businesses consider one cloud to be equal to the next and providers to offer equal services, with the same levels of security and service options.

This is not the case. Reputable Cloud providers do offer enhanced security compared with the security many businesses are able to achieve in-house. However, this is not a guaranteed service from all cloud providers. Security, reliability and service level agreements will differ from one provider to the next and it is important to ensure due diligence is undertaken to avoid disappointment or risk.

Conclusion

One of the biggest barriers to cloud adoption, without a doubt, is security. Yet cloud security continues to evolve as confidence grows and the adoption of cloud technologies expands across the globe.

It's safe to suggest that most businesses will not be able to come anywhere close to handling security better than a large cloud provider with the uninterrupted resources, dedication and the expertise necessary.

Cloud tends to be a great security advancement for many businesses of all sizes. Yes, security risk is present but the risk is present if we choose not to work in the cloud as well. What is important is to be knowledgeable of the actual security risks so that we can place focus where required, thus enabling us to manage security in the most appropriate manner possible.

Reduce Risk

- Improve behaviour
- Share security responsibility
- Reduce business risk

Meet Compliance Requirements

- Implement best practise
- Meet compliance objectives

Make More Money

- Reduce infections and related costs
- Free up resources to improve productivity