RMS
The Hospitality Cloud

A complete guide to Data Security and what questions you should be asking.

Introduction

Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly important because the data is located in different places.

Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Organizations use the cloud in a variety of different service models (with acronyms such as SaaS, PaaS, and IaaS).

Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.

The purpose of this document to provide you with the correct information and encourage you to ask your provider to prove they comply with the industry standards.

Data Centre and Server Room Standards

All Data centres, regardless of where they are located, should have a Policy Statement, you can ask your provider to produce theirs, this is particularly important if they have built their own data centre. The purpose of the Data Centre and Server Room Standards is to describe the minimum requirements for designing, installing, securing, monitoring, maintaining, protecting, and decommissioning a data center or server room.

This, seemingly simple document, could mistakingly be overlooked to those not in-the-know. The comprehensive policy statement should cover topics such as CRAC (Computer Room Air Conditioner), Humidity/temperature control, Cooling Towers, Electrical System, Maintenance, Testing, Access Control and Safety. As well as the structural aspects ie. Raised floor systems, Server cabinet systems and even the frequency and equipment to be used during the cleaning process, as dust, moisture and heat can severely impact the efficiency of the servers and, in turn, your data. Your provider should have no problem answering all your questions, or providing documentation.

Data Centre Structural Integrity

Data centre facilities should, as standard, be located in a secure, private location with extensive 24 hour security and advanced structural integrity. To achieve the level of sophistication required for a truly secure data centre, choosing internationally recognised, government-level security companies, such as IBM Softlayer is highly recommended. To give an example of the advanced and complex level of security they provide, and you should expect from your own provider, here is an excerpt from IBM Policy:

> *"Facilities are specifically designed and constructed to sustain a seismic event while maintaining business functions and boasts low latency through superior connections to robust fiber optic loops, 55mW of existing electrical capacity, 45 on-site generators with .5-million gallons of on-site fuel storage, and a carrier vault system supported by more than 50 miles of embedded, secure conduits."*

Security Assessment and Testing

It is vital your Data Security supplier is not only certified meeting the industry-recognized requirements, eg. SSAE16 (SOC1) certified, but also undergoes extensive intrusion testing, by an independent third party. This exhaustive, third-party certification assessment should include, but is not limited to, the extensive testing of the control objectives and activities at all data centre facilities, including oversight by executive management, operations and customer service, development and information technology organization, human resources policies and procedures, and risk assessment monitoring.

Intrusion testing, also known as penetration testing, is also a vital element of the security process. This should be conducted regularly and by an independent third party security assessor. Through the application of rigorous methodologies, the use of automated scanning tools, customised proprietary scripts and manual techniques, your provider should be tested for exploitable vulnerabilities that could allow unauthorized access to key information assets.

Most reputable data-security suppliers will supply redacted reports summarising the methods and methodologies used, on request.

Data Breach Response Plan

Any company worth your data should have an up-to-date accessible Data Breach Response Plan that clearly states the Response Team, their roles and responsibilities, and outlines the procedures to be undertaken in the event if a data breach. Most companies will have this on their website.

PCI Compliance

Payment Card Industry Data Security Standards (PCI DSS) refers to the global information standard set by the payment card industry to assist with the prevention of payment card fraud. To achieve compliance, a company must successfully demonstrate it has met stringent measures in enforcing the data security of the companies with which it conducts business. All reputable companies will have their up-to-date PCI DSS Certificate of Compliance readily available, and most often on their website.

Examples of questions for your Data Security Supplier:

- Are your Data Centres SSAE16 and ISO 27002 industry-recognised Certified?
  (These are the certificates that deal with the infrastructure)
- Can you provide the certification?
- Where is your data stored?
- What data storage company, if any, are you using? (eg. IBM/Softlayer)
  Why? / Why Not?
- Can you provide a Data Policy for each of your data centres?
- What form of intrusion testing is preformed and how frequently?
- What third party assessors are used, can you supply up to date certification?
- What is the back-up policy of your data centre?
- What are the response procedures for a breach?
- Can you provide your PCI Compliance certificate?

Don’t Take It For Granted

The above are just a few examples of questions you should be asking, too often it is taken for granted that companies responsible for your data security are fully compliant and have met all the industry standard requirements. If a company has all of the above mentioned they will will have no issues answering all your questions and presenting the relevant information.

So whether you are an existing customer or looking to change PMS provider, be sure to protect your company and it’s sensitive data by asking the right questions.

Examples of Best-In-Industry Security Certificatons

www.rmscloud.com
03 8399 9462
sales@rms.com.au