Cloud computing 101
Getting clear about the cloud

CNA
We can show you more.®

TECHNOLOGY

Cloud computing is a growing trend in information technology as organizations look for ways to save money and an appealing alternative to the way they interface with data and applications, such as email and customer databases. But what, exactly is "The Cloud?" This brief paper will help you understand the benefits of working in the cloud and provide you with some insight about risks associated with cloud computing.

What are the benefits of the cloud?

Cloud computing, while still an evolving service, provides on-demand network access to a shared pool of computing resources, such as networks, servers, storage and applications. This means that by using a cloud provider, your company, customers or clients can access information, files or data anytime, anywhere from virtually any device with an Internet connection. The pooling of resources allows rapid scaling to meet your company's changing needs.

In contrast to buying and installing software onto your existing hardware or having to procure new hardware or servers, cloud computing can provide a cost-efficient alternative. Companies have gained tremendous flexibility and agility in rapidly scaling their resources up or down on an "as needed" basis. Beyond the heightened accessibility and ease of collaboration, the potential cost reductions can be significant. In short, the cloud is an instrument that can vastly simplify, optimize and streamline the way your organization's IT operates.

Different clouds for different crowds.

There are four basic types of cloud services that may be available to your organization:

Public: Public clouds make applications and storage available to the general public. The cloud infrastructure is owned by the cloud provider, and services may be purchased on a pay-per-usage basis.

Private: Private clouds are dedicated to a single organization. This option can be more expensive, but does offer enhanced privacy, data security and control. They can exist on or off premises, and can be managed internally or by a third-party service provider.

Community: Community clouds are shared by multiple organizations that have common concerns, such as similar security, policy and compliance requirements. Government entities or hospital groups may find community clouds an efficient means of combining assets and sharing resources.

Hybrid: Hybrid clouds are comprised of two or more types of clouds. Critical activities are usually performed via a private cloud, whereas non-critical activities might use a public cloud. They are hosted with a mix of internal and external services

Storing data in the cloud? Know the risks on the ground.

As with all emerging technology solutions, companies must make sure they address potential risks when operating in the cloud. Cloud solutions are complex networked systems, which are affected by traditional computer and network security issues such as the data confidentiality, data integrity and system availability.

Some of the key risks that your company should examine include:

Data Protection: A data breach can devastate a company, which can make placing sensitive data in the hands of a third party unsettling. Ensuring that your data remains secure and protected while at rest and in transit is paramount. Encryption is one way to safeguard your company's data. To further safeguard confidentiality, encryption keys should be owned and managed solely by the cloud customer.

Data Loss/Disruption: Damage from storms, natural disasters or an electrical failure can potentially cripple a data center. Other incidents like fire or a water leak can pose damage to servers. And even if your provider has a recovery process, there's the chance that your data may still be irretrievable.

It's important to have a contingency plan in place should a disruption or loss occur. You need to know how easily your critical data can be retrieved and identify a new provider or non-cloud space in which to transfer data.

Inappropriate Access: Data that rests in the cloud should be accessible only by those with distinct authorization. The vast amount of data and users makes the cloud environment extremely alluring to hackers. And you can't rule out an ex-employee who can still gain access.

Stringent user authentication can help block inappropriate users from infiltrating your cloud space and accessing data. Companies should consider viewing access logs and audit trails for added user verification.

Are you ready for the cloud?

At CNA, we stay ahead of the technology curve, developing coverages and services that quickly respond to emerging risks and global exposures for virtually any industry. If your company is considering a cloud-based solution, you need insurance that will put your mind at ease and a carrier that will help you manage your risks.

Cloud "lingo" you should know.

Software as a Service (SaaS):
Provides ready for use Web-based applications such as email that are maintained centrally by a provider (e.g., Gmail, Salesforce.com).

Platform as a Service (PaaS):
Provides programming languages and tools that can be used by application developers to create and deploy applications on the Web. These platforms inherently supply the infrastructure, connectivity and security needed for development, which means less time, money and manpower spent by your organization.

Infrastructure as a Service (IaaS):
Provides computing resources, such as virtualized servers and storage, whose usage is rented from a provider (e.g., Amazon EC2, Windows Azure). This structure is a fully outsourced, on-demand, pay-per-usage approach to computing resources, data storage, network and operating systems. You're able to deploy, run and control software, without having to physically purchase hardware or software.

To learn more, contact your local independent agent or visit www.cna.com/technology.