Chubb Risk Bulletin:

Security in the Cloud

CHUBB®

If your company does not already have applications, data, or infrastructure in the cloud, you are probably considering it. The use of the cloud can provide cost saving, scalability, flexibility, and access to robust infrastructure, but will it be secure and reliable? What is the risk to your organisation, and how do you evaluate it?

What is Cloud Computing?

Cloud computing is a model for enabling convenient, on-demand access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing can be in a private cloud, a public cloud or a hybrid.

Private clouds, also called an internal cloud or enterprise cloud, offer activities and functions 'as a service' but are deployed over a company intranet or hosted data center. A private cloud is intended for a company or organisation with advanced security and highly available or fault tolerant requirements. This level of security and control is generally not possible in a public cloud model. Subsequently, private cloud owner shares few, if any, data or other virtual assets with other organisations. This approach requires more internal resources, but provides a significant level of internal Information Technology (IT) management.

Public clouds, also known as a shared cloud, are provided 'as a service' over the internet with little or no control over the underlying technology infrastructure. This approach is cost effective and provides rapid IT deployment, but cedes control of information security to a third-party.

Hybrid clouds are a composition of cloud models (private, public, etc.) that remain unique entities but are bound together by standardised or proprietary technology that enables data and application portability (e.g. cloud bursting for balancing between clouds).

Chubb Risk Bulletin: Security in the Cloud, Australia. Published 03/2019.

Cloud services broadly fall into three service models:

- **Software-as-a-Service (SaaS)** - allowing a consumer to use a cloud provider's software applications that operate on the provider's infrastructure.
- **Platform-as-a-Service (PaaS)** - allowing a consumer to deploy applications it creates or acquires onto cloud infrastructure using the cloud provider's programming languages and tools. With PaaS, the consumer controls the application but not the underlying infrastructure.
- **Infrastructure-as-a-Service (IaaS)** - allowing a consumer to run operating systems and applications on a cloud provider's infrastructure. IaaS is like renting an IT department owned and operated by a cloud provider.

Regulatory Environment in the Cloud

Australian organisations and cloud service providers of Australian organisations are subject to the requirements of the Privacy Act 1988 (the "**Act**"). The Act is intended to regulate how personal information is collected, handled and protected, and applies to Government Agencies, private health service providers, private sector and not-for-profit organisations with annual turnover greater than $3 million, and some small businesses. International regulations such as the EU General Data Protection Regulation (GDPR) may also apply if your organisation is operating in the cloud in the EU, or providing cloud services in the EU.

The Privacy Act 1988 sets out obligations for the handling of personal information in the form of thirteen Australian Privacy Principles (APPs). When operating in the cloud, it is necessary that your organisation and the cloud service provider conform to these APPs, amongst other legal and regulatory requirements. This is particularly important to consider when using cloud service providers which operate overseas, or if your organisation shares cloud information with an international parent company or subsidiary. A full list of the APPs and their requirements is available on the Office of the Australian Information Commissioner (OAIC) website.

From 22 February 2018, the Privacy Act 1988 introduced the Notifiable Data Breaches (NDB) scheme. The NDB scheme applies to organisations covered under the Act and applies to data breaches involving personal information that is likely to cause serious harm to affected individuals. When an eligible data breach is suspected, organisations are obligated to notify affected individuals and the OAIC. When storing personnel information in the cloud, it is important to assess how this information is protected from unauthorised access and/or disclosure, and how your organisation and cloud service provider will identity and respond to data breaches, amongst other considerations.

In Australia, many regulators take an interest in cloud computing, from the OAIC to the Australian Regulatory Prudential Regulation Authority. As the regulatory environment for cloud computing is constantly changing and varies throughout the world , it is recommended that legal, risk and compliance counsel are consulted, especially when your cloud operations extend outside of Australian borders.

Threats in the Cloud

When compared to traditional on-premise computing, cloud computing requires subscribers to give up (to providers) important capabilities, such as:

- **Control** - Depending on the cloud model (private vs. public vs. hybrid), you as the subscriber hand over control of your data, applications and/or infrastructure to a third party provider. Public clouds are designed to host IT functions and assets on the cloud vendor's servers and within their building or leased datacentre space. You may have little control over system security, provided with only a few options related to access management and data encryption. You must trust in the reliability and competence of your provider.
- **Visibility** - Depending on the cloud model, you may not even know where your application and data are being stored, let alone details on the cloud provider's security and infrastructure. Access to internal and external information security audits can increase visibility, but cloud providers are not always amenable to sharing that information. A right to audit clause in the SLA, Service Level Agreement, can pave the way to increased visibility.

With the above in mind, it is important to consider cloud computing threats. The following threats should be considered at a minimum when operating in the cloud:

- **Data Theft** - Theft of confidential corporate information is always a risk to any IT infrastructure, but the cloud model offers new avenues for cyber-attacks. If the base of the cloud data from multiple clients is not thought out properly, a flaw in the application of one client can open attackers' access to data not only of the client, but all other clients.
- **Loss of Data** - The data stored in the cloud, can be removed or destroyed by hackers or lost for other reasons. Data storage devices can suffer a fire or natural disaster, or data can be accidentally deleted if a provider of cloud services does not introduce proper backup measures.
- **Service Traffic Hijacking** - In a cloud environment, an attacker could use stolen login information to intercept, forge or give distorted information or redirect users to malicious sites. Organisations should prohibit distribution of their login information for all services. A robust, two-factor authentication may reduce the risk.

- **Insecure Interfaces and API** - Organisations are subjected to a variety of threats if they use weak interface software or Application Programming Interfaces (APIs) to manage and interact with cloud services. These interfaces must be well designed and secured to include at a minimum authentication, access control and encryption.
- **Denial of Service** - The cloud can be vulnerable to attacks such as a denial of service attack (DoS-attack) which can cause infrastructure overload, consume large amounts of system resources and prevent customers from using the service. Media attention often involves distributed DoS-attacks (DDoS-attacks), but there are other types of DoS-attacks which can block the cloud usage.
- **Malicious Insiders** - Without proper level of security on IaaS, PaaS or SaaS, an insider who has improper intentions (e.g., system administrator) may gain access to confidential information that is not intended for them.
- **Lack of Foresight** - In pursuit of cost savings and other benefits of the cloud, some organisations rush to use cloud services without considering the information security implications. Organisations should conduct a comprehensive, thorough review of its internal systems and potential cloud providers to fully understand all the information security risks before moving to a new model.

Resources

www.cloudsecurityalliance.org
CSA Top Threats to Cloud Computing V 1.0, March 2010 CSA Security Guidance for Critical Areas of Focus in Cloud Computing V 3.0, 2011

www.csrc.nist.gov
NIST Special Publication 800-146, Draft Cloud Computing Synopsis and Recommendations, May 2012 NIST Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011

www.oaic.gov.au
Office of the Australian Information Commissioner

Connect With Us

For more information about Chubb's cyber policies to protect SMEs, contact your local Chubb Risk Engineer or visit our website.

About Chubb in Australia

Chubb is the world's largest publicly traded property and casualty insurer. Chubb, via acquisitions by its predecessor companies, has been present in Australia for almost 100 years. Its operation in Australia (Chubb Insurance Australia Limited) provides specialised and customised coverages include Marine, Property, Liability, Energy, Professional Indemnity, Directors & Officers, Financial Lines, Utilities as well as Accident & Health, for a broad client base, including many of the country's largest companies.

More information can be found at www.chubb.com/au

Contact Us

Australia Head Office
Grosvenor Place
Level 38, 225 George Street
Sydney NSW 2000
O +61 2 9335 3200
F +61 2 9335 3411
www.chubb.com/au

Queensland office
Waterfront Place
Level 30, 1 Eagle Street
Brisbane QLD 4000
O +61 7 3221 1699

South Australia office
Level 7, 147 Pirie Street
Adelaide SA 5000
O +61 8 8418 3000
F +61 8 8418 3010

Victoria office
Level 12, 720 Bourke Street
Melbourne VIC 3000
O +61 3 9242 5111
F +61 3 9642 0909

Western Australia office
Level 18, 44 St George's Terrace
Perth WA 6000
O +61 8 9325 2399
F +61 8 9221 1559

Chubb.Insured.℠