



Liberty Technical Update 8 - Cloud Computing

Cloud Computing and Insurance Risk Management

If you are in the Information Technology (IT) or telecom industry, you would be familiar with the concept of “Cloud Computing” – a concept that has been bandied about for the past couple of years. But what precisely is “cloud computing”? How does it work and what does it mean for your business from an insurance risk management perspective? This Technical Update examines these issues and highlights some of the risk management concerns that need to be borne in mind.

What is “Cloud Computing”?

Put simplistically, cloud computing is a broad term used to describe technology services delivered over the Internet. Webmail and online documents (such as Google Docs) are well-known examples. Instead of a user of IT services storing or accessing computing technology services via a server that is physically located in their office, cloud computing services allows their necessary data to “live in the cloud” – on a different physical server, in another place, not usually owned by the same business - providing platform, software or infrastructure solutions. Computer processing and data storage services, for example, known as “infrastructure as a service”, provides businesses with access to their servers to store and process data. Software that provides a range of tools to help build and run applications on servers, known as “platform as a service”, is available as part of cloud computing services as is the delivery of applications over the Internet, otherwise known as “software as a service”. All these services and applications are hosted on and accessed through the Internet wherever and whenever they are required by the customers.

One key advantage of cloud computing services is the fact that they are elastic and scalable. This means that the extent of the services and resources can be scaled up or down depending on the customers’ requirements. Businesses do not have to outlay enormous capital expenses on hardware or software based on anticipated needs. Instead, they buy the relevant services on a subscription basis. The other benefit is that companies do not need to have actual space in their offices to house the necessary infrastructure. An example of the benefit of cloud computing can be seen from the recent terrible flooding in Queensland.

Some businesses that had cloud computing services and whose office premises were flooded were still able to operate through their mobile telephones, laptops etc. for their computing requirements.

Key Exposures in Relation to Cloud Computing

If you are a cloud service provider, then your service agreements with your customers should address key issues such as: the standard of service to be delivered and the consequences of denial of access or non delivery (eg. what if the Internet is unavailable?), liability regimes (eg. what is the extent of your liability in relation to customers’ loss of business continuity?), security standards and the consequences of a breach of security, ownership of intellectual property, warranties and indemnities provisions and termination clauses.

In addition to these important issues, however, the following must also be addressed:

Privacy and Confidentiality

Any information that can be stored locally on an office computer can be stored “in the cloud”. This means that valuable information that is contained in emails, word processing documents, spreadsheets, health records, tax or other financial information, business plans, sales numbers, trade secrets and other confidential information could be stored in the cloud. If the cloud services are made available to customers over the public Internet (otherwise known as the “public cloud”) then the data is stored outside the customer’s own firewall. What are the legal and financial exposures of a cloud service provider when such private and personal information is leaked to or accessed by third parties? While some customers may require the security of “private clouds” (where the virtualized cloud data centres are inside the customer’s own firewall or a private space is dedicated to the customer within the cloud provider’s own data centre), stringent security standards are still needed in order to safeguard the private and confidential information of customers who may have legitimate concerns about their data security.

“Cloud computing services allows your data to “live in the cloud”
- on a different physical server in another place.”



Proper internal policies in relation to privacy protection are crucial and, from a legal risk management perspective, careful contractual management of security standards and the consequences of security breaches are important elements to consider. They have not only commercial but reputational implications for your business.

Compliance across Multiple Jurisdictions

This is another key exposure that merits attention. The geographical location of information that is stored in the cloud may have significant effects on the privacy and confidentiality protections of the information and on the privacy obligations of those who process or store that information. The point is that any information stored in the cloud eventually ends up on a physical machine owned by a particular company or person located in a specific country. That stored information is likely to be subject to the laws of the country where the physical machine is located. For example, personal information that ends up being maintained by a cloud provider in a European Union Member State could be subject permanently to European Union privacy laws. Similarly, if that information is stored in Singapore, where there is currently no legislative privacy regime, the cloud service provider could be subject to those laws. At the same time, the cloud service provider may be in breach of its privacy obligations to its Australian customers who would expect privacy and confidentiality protection in accordance with the Australian National Privacy Principles. If a customer is based in Australia but the information in the cloud is stored in Singapore, a cloud service provider may need to ensure that client information is properly protected so as to comply with Australian privacy law requirements.

Furthermore, what if the data that belongs to a client is information that cannot be stored offshore? For example, Australia's Australian Prudential Regulation Authority (APRA) regulates the financial sector in Australia. One of the requirements is that financial services companies (such as financial institutions and funds managers) that wish to transfer data offshore may first need to notify APRA and demonstrate to the regulator that appropriate risk management procedures have been put in place to protect such data. A failure to do so may result in a breach of licensing requirements which could result in financial loss for the financial service provider and their customers.

If you are a provider of cloud services to Australian financial institutions or regulated entities, you need to bear this in mind when negotiating contracts for cloud services to ensure that all contracting parties understand the risks involved in the proper storage of data and how to manage risks so as to ensure legal compliance.

Errors and Omissions Liability Insurance

Consider the scenario above: suppose a funds manager brings a claim against their cloud service provider for loss of revenue due to the loss of its licence as a result of the fact that data belonging to their customers have been transferred offshore without satisfying APRA's requirements for data protection. Is the funds manager covered in respect of their customer's loss of revenue? What about a breach of privacy claim that has been made against the fund manager who in turn brings an indemnification claim against their cloud service provider? If your company is a cloud service provider, it is essential that you talk to an insurer who has a good understanding of the risks associated with cloud computing services and who can discuss with you the pertinent issues with a view to finding insurance solutions for them. LIU has designed E&O liability policies which cater specifically to the commercial needs of those in the IT or telecommunications industry.

From a financial risk management perspective, proper insurance protection for the legal liability risks associated with cloud computing services is vital.

This information is presented by Liberty International Underwriters, the trading name of Liberty Mutual Insurance Company, ABN 61 086 083 605 (Incorporated in Massachusetts, USA. The liability of members is limited). It is a general comment only on the subject matter, and should not be relied upon as advice or any definitive statement of law in any jurisdiction. Obtain your own professional advice before applying this to your circumstances. This information is current as at November 2011.



Please Contact Richard Head on + 852 3655 2623 or visit www.liuasiapacific.com