

Data breach and risk in the Cloud - the legal response

by Thomas J. Shaw, Esq, attorney at law, and CEO, CloudRisk Asia

With increasing likelihood of a serious data security breach, enterprises moving to the Cloud need to consider their responses - technical response with data recovery; response to business and reputation damage-limitation; and legal responses. Organisations whose systems are breached must notify customers when 'real risk of harm is reasonably foreseeable'. Data breaches notifications are prescribed by regulations or guidelines in most Asia-Pacific (APAC) countries. These regulations specify who should notify whom, in what circumstances, what was breached, whose data was breached, etc. Enterprises should prepare for such eventuality, assess the risk and manage them continually.



Thomas J. Shaw, Esq. is an attorney at law, CPA, CRISC, CIP, CIPP, CISM, ERMP, CISA, CGEIT and CCSK. He is based in Asia and works with organisations globally on data privacy, information security, e-discovery/litigation readiness, Cloud computing, social networking, e-commerce, intellectual property, transactional law, compliance, information governance, outsourcing and technology risk assessment. He speaks and writes frequently on information and Internet law and technology.

Mr Shaw is the author of several books. In 2012: Children and the Internet - A Global Guide for Lawyers and Parents; in 2011: Cloud Computing for Lawyers and Executives - A Global Approach; and in 2011: Information Security and Privacy - A Practical Guide for Global Executives, Lawyers and Technologists. He is editor/frequent author of the American Bar Association publications covering the latest developments in technology and law: the Information Security and Privacy News and the E-Discovery and Digital Evidence Journal.

Mr Shaw runs CloudRisk Asia, which provides risk assessment to corporations and their Cloud service providers. He develops and delivers Cloud computing risk workshops.

There is growing excitement about the benefits of Cloud computing, which are visible every time one sends an Internet email, saves a file in their Internet storage, participates in a social network, or outsources processing resources. So why is not every organisation committed to fully deploying the Cloud? One reason is that there are legacy hardware or software resources that have not reached the end of their economic lifecycle. There are also regulators preventing participants in certain industries from moving more fully into the Cloud. More likely, it comes down to simple FUD (*Fear, Uncertainty and Doubt*). The FUD factor predominates partly because Cloud computing has been ushered in with such a tidal wave of marketing hype. Nothing so hyped can be really this good, can it? Beyond the fear and the hype, experienced IT personnel know that there may be new risks when computing capability is moved outside of their direct

control. It is these risks of Cloud computing services that the article addresses.

Governments across the Asia-Pacific region are making efforts to promote the use of the Cloud, through funding infrastructure or deploying their own Clouds, encouraging the setting of standards and providing awareness education and training on the Cloud. While there are clearly differences in how far countries have gone in developing the Cloud, users of Cloud computing services will all face a similar set of risks when utilising the various services of Cloud Service Providers (CSPs). This includes both public and private-sector organisations and those firms which outsource to the public Cloud and those which in-source to a private Cloud or do both with a hybrid Cloud.

These risks of Cloud computing can be grouped into six categories:

- Legal: the sum total of all legal obligations an organisation is subject to, from all Cloud-related statutes around the world.
- Data protection: how prepared are those responsible for keeping Cloud data safeguarded.
- Contracting: how well is the organisation legally protected against undesired Cloud events.
- Governance: how easily can data be safely moved within and between CSPs.
- Verification: what independent third-party assurances are provided about the CSP.
- Response: how prepared is the CSP to handle security-related incidents.

Explanation of all of these Cloud-related risks takes up a whole chapter in my Cloud computing book, so here I will focus on part of a single risk, within the category of response risk, regarding the preparation for and response to a data breach in the Cloud.

Historically, organisational data resided in closed networks, inaccessible from outside. With the migration to the Internet and Cloud computing, data is collected over the public network and stored on devices accessible via the Cloud. The growing threats from bad actors and the vulnerabilities inherent in using an open network combine to present a set of risks that have manifested themselves everywhere. The list of publicly known organisations (e.g. Sony, Citigroup, Honda), less-well known organisations (e.g. Global Payments, Heartland, Hannaford Bros.), Cloud-based systems (e.g. Nasdaq, Epsilon, CheckFree), and firms dedicated to security (e.g. RSA, VeriSign, DigiNotar) known to have had their data/networks breached in the last several years is already large and still growing.

While some of the data breaches are of more concern than others, the reality that all organisations should accept is that it is more likely than not that they will experience a data breach of some kind. The question then becomes, how will your organisation respond to a data breach event, especially after data has been migrated to the Cloud?

There are three distinct aspects to data breach response:

- a) The technical response: how to identify the incident, how to quarantine the intrusion to prevent further damage, how to repair all infected systems, how to restore the appropriate data, and what are the appropriate reviewing and remedial actions to ensure this type of incident does not recur.
- b) The business and reputational response: attempting to limit the impact on the entity's financial viability, revenue loss and damage to trademarks reputation and brand names, including minimising related costs and seeking insurance pay-outs.
- c) The legal response: getting law enforcement involved, when organisations must comply with a variety of statutory and regulatory requirements, which potentially requires certain evidence to be locked up or frozen. The following looks at these legal aspects of a data breach response.

Across the Asia-Pacific region, there are a variety of laws concerning the response to a data breach. Many of these general provisions at this time are voluntary guidelines, although certain industries are required to report breaches, at least to their regulators. For example, in Australia, there is no general data breach statute but there are voluntary guidelines from the government. In Hong Kong, the proposed changes to the local privacy ordinance will make the breach notification

process voluntary, but the government has published guidelines and templates in advance of those changes. Japan has industry sector regulations regarding data breach notification. In Taiwan and South Korea, newer revisions to their privacy laws require data breach notifications. There are local versions of data breach laws arising in China, to complement national breach notice regulations on service providers.

In Europe, under the e-Privacy Directive, member states are required to implement local legislation where service providers that are responsible for hosting and transmitting customer's data are required to notify the appropriate national authorities upon the event of a data breach. If an end-customer's breached data can negatively impact on them, they must be notified as well. By contrast, in the US, while there is no general federal data-breach notification requirement, there are industry sector specific regulations in healthcare and financial services for reporting of data breaches and there are general data-breach notification laws in almost every state.

These laws require that organisations whose systems are breached and expose their customer's data to the risk of harm to notify customers if the data could be used maliciously. This is most typically the case when the data is personally identifiable information or financial information, kept in an unencrypted format. What typically varies among these laws is the information that must be reported, to whom it must be reported, and when it must be reported. The data breach legal response when data is outsourced to the Cloud will essentially come down to answering a series of questions:

- What data breach and privacy laws are implicated by a CSP data breach, as the data servers and customers may be situated in disparate countries around the world?
- Who is going to report the data breach, the CSP or the CSP's customers whose data was breached?
- When must the breach be reported, after an investigation or as soon as it occurs, or perhaps never?
- To whom must the breach be reported to, such as to: the local data protection authorities, industry regulators, local and/or international law enforcement (e.g. Interpol), department of justice agencies, and/or to the data owners or their data custodians if outsourced?
- In what circumstances must the data breach be reported, such as when: a certain number of records have been breached, a certain type of sensitive data is breached, or criminal activity is suspected?
- What types of information has to be reported?

- How does the CSP know, in a virtual-resource multitenant Cloud environment, just whose data has been breached?
- What type of evidence has to be saved for future criminal investigations or civil litigation, such as logs of the network and system activity or images of before and after data, and how can this be done in a multi-tenant Cloud environment?

While a comprehensive example is beyond the scope of this article, the guidance from the government of Hong Kong provides insights into part of the legal response. The guidance suggests that the data custodian first gathers information, including when and where the breach occurred, how it was detected, what the cause was, what type of personal data was affected and the number of data subjects potentially impacted. It advises notifying data subjects when the 'real risk of harm is reasonably foreseeable'.

The breach notification should include:

- date and time of the breach and its discovery;
- the cause of the breach, the personal data breached;
- the potential risks of harm;
- the remedial measures to ensure no further data loss;
- a contact person and number;
- the law enforcement or other agencies notified;
- what is being done to assist affected consumers;
- and, what they can do themselves to mitigate the risk of harm, such as identity theft and financial fraud.

The important lesson here is that when moving data into the Cloud, organisations must recognise that they are (possibly) taking on more risk of their data being breached. To address this, they must take several essential steps to counter-balance that risk. These are to:

- risk assess both themselves and any CSPs that they use;
- implement appropriate risk treatments to manage those risks;
- continually monitor the effectiveness of the risk treatments to identify new risks;
- proactively develop a data breach response plan.

The Cloud remains the future of IT but assessing its risks and proactively preparing for the worst is the best practice for organisations, in Asia and elsewhere around the world. Advance planning for data breaches within the Cloud is the most prudent course of action for all types of organisations. ●