This article was published in the August 2017 issue of the
Singapore Law Gazette, the official publication of the Law Society of Singapore.

Navigating to the Cloud: A Framework for Trust

Jennifer Koo
Microsoft Singapore
E-mail: jekoo@microsoft.com

Introduction

As we stand today on the cusp of the Fourth Industrial Revolution, the legal service industry, like all modern industries, is reaching a point where innovation is no longer an option. To stay ahead in a highly competitive market, law firms must keep up with technology. In this digital era that has seen great advancements in artificial intelligence, natural language processing, and data analytics, the on-demand resourcing provided by cloud computing provides a compelling foundation for the business of law. The economic and strategic advantages of cloud computing make it impossible to ignore – the cloud can help law firms save money, reduce complexity of IT process, improve operational efficiency, increase the mobility and productivity of lawyers, and, assuming a law firm is working with a trusted cloud services provider ("**CSP**"), enhance the security of client data.[1] The issue therefore is not whether to move to the cloud, but how to do so safely and within the bounds of the lawyers' ethical and professional obligations.

Starting the Journey to the Cloud

A critical first step to successful cloud adoption is to understand the technology. Law firms do not have to turn into cloud experts. There is a view that, to competently represent their clients, law firms must keep abreast of changes in the law and their practice, including the benefits and risks associated with the relevant technology.[2] Understanding the cloud will help law firms make informed decisions about the deployment models and service delivery models that are appropriate for their needs and

risk tolerance.[3] For example, law firms that need to retain certain type of information on-premises can choose a hybrid solution for having certain data on-premises and the rest in the cloud.

Second, law firms must identify the use cases for the cloud. Not all technology is right for every situation, but business scenarios that cannot benefit from the cloud are few and far between. The approach of the UK Government is instructive. In addition to describing cloud-suitable scenarios, the UK Government has implemented data classification to understand the actual and perceived risks and needs regarding storage on cloud or on-premise.[4] Data classification policies are therefore essential to both help law firms comply with data storage controls, and to identify the right technology for different scenarios for optimal resource utilization. Another emerging use case for cloud technology is to help mitigate cybersecurity threats. CSPs can employ security processes and protocols, including constant updates and patching to tackle the newest and most invasive security threats that are beyond the means of most law firms. This is because security is a critical aspect of the business models for most reputable CSPs, and considered a core competency.

Third, law firms must understand the regulatory landscape for the adoption of technology, and identify key risks and mitigation strategies. A pertinent question is whether the use of cloud services is consistent with the rules on professional conduct. There is a view that lawyers may use cloud services to create, transfer and store client-related data so long as they take reasonable steps to ensure that such information remains secure and protected.[5] The issue of whether privilege can withstand the modern cybersecurity threats is not a subject for this paper, but recent case laws suggest that courts will not place unwitting victims at a significant disadvantage in the court process.[6] In addition to rules on professional conduct, other laws may also apply, such as the Personal Data Protection Act ("PDPA").

The Challenges of the Cloud: A Risk Evaluation Framework

The crux of the challenges of the cloud lies in the fact that organisations who are often subject to stringent regulatory requirements must entrust sensitive data or the mission-critical business applications that process this data, into the hands of third parties whose facilities they do not control. In addition to assessing the CSP's reputation, competence and flexibility of service offerings, it is important to use a meaningful risk evaluation framework, such as the following that is based on four key principles of trust: security, privacy and control, compliance, and transparency.

Security of Data in the Cloud

Although many of the threats that face cloud environments are the same as those for traditional corporate networks, security remains one of the biggest concerns with cloud adoption. This is because organisations assume increased risks arising from moving data over the internet, storing data with an external organisation, the possibility of access by employees of that organisation, and the perceived attractiveness of cloud environments to hackers. However, there is increasing consensus that the cloud may offer stronger security advantages that on-premises systems and in-house capabilities cannot match. Today, security (rather than cost) is increasingly becoming the key driver for organisations to move to the cloud.

To comply with their legal obligations, lawyers need to consider whether the CSP has implemented appropriate and reasonable security measures. Law firms must expect a level of security in the cloud environment as being on par with or better than the security provided by their non-cloud IT environment. CSPs must provide assurance that they will implement strong and up-to-date security practices that meet or exceed international standards, to prevent both unauthorised insiders and outside hackers from being able to access the data. Examples are:

1. robust encryption to prevent unauthorised access to data, at rest or in transit;
2. implementation of policies and controls for governance and management of information security;
3. monitoring and logging technologies for visibility into the activities on its cloud-based network;
4. strict access controls over personnel who may be granted access to customer data;
5. incident response processes;
6. data isolation and segregation so that the data cannot be accessed or compromised by co-tenants in a multi-tenanted environment; and
7. Hardened physical systems, including 24-hour monitored physical hardware.

Law firms should ensure that the cloud service agreement contains binding commitments as to critical security features of the cloud services. The cloud service agreement should also address what happens in the event of a data breach incident – including any applicable notification, investigation and mitigation protocols.

As most CSPs will rely on the use of sub-contractors to provide certain support services, law firms should also

ensure continued legal and regulatory compliance no matter who holds the data or provides the services. This can be done by way of requiring contractual commitments from CSPs to take responsibility for compliance, and to ensure that their subcontractors are subject to protections and controls that are equivalent to those applied by the CSPs themselves. The CSP should share details of its sub-contracting arrangements, including providing a list of its sub-contractors, and ensure that there is a mechanism to notify the law firms of any updates to the list.

Privacy and Control of Data in the Cloud

Concerns with the challenges arising from losing control over data in the cloud are understandable and should be addressed. Even though the data is being stored off-premises in the CSP's data centers, law firms still need to remain in control of its data. In addition to technical means to assert control that may be provided by the CSP, the principles of data ownership, and how much say the law firms will have over the use of and access to the data are crucial to consider. The law firms must ensure that the CSP agree contractually that the law firms retain ownership of their data, and that the data will only be used in ways that are consistent with their expectations. The CSP must not have the rights to use the data for any purpose other than of providing the cloud services, such as advertising or similar commercial purposes. It is worth noting that Singapore data protection laws prohibit personal data from being used for secondary reasons other than the purpose for which it was originally collected.

Given the increasingly stringent laws in many countries relating to personal information, law firms should seek a broad commitment from CSPs that they will deal with personal information in accordance with applicable privacy and data protection laws. Obligations undertaken by the CSP should be aligned to the strictest benchmark of privacy requirements, such as the EU laws. Law firms should know the locations of the data to ensure that the requirements of applicable data protection and privacy laws are followed. For example, the PDPA requires the imposition of legally enforceable obligations comparable to the PDPA standard of protection, on a recipient outside of Singapore and EU laws requires the transfer of personal data outside of EU to be handled in very specific ways. It is also important that CSPs contractually commit not to disclose any data to third parties, unless with the law firms' consent or when required by law. CSPs must be clear on the steps that they will take when they receive requests or demands from law enforcement for law firm's data. These should include a commitment to redirect the request to the law firms, unless prohibited by law. To maintain security and confidentiality of the data, law firms must also ensure that their data will be segregated from the data of other customers of the CSP. Data segregation also helps make termination easier to deal with since data can be more easily returned and deleted.

Law firms must ensure appropriate exit process provisions are included and adequately documented in their cloud service agreement. Law firms must be clear about what happens to the data at the end of the relationship with the CSP. During the exit process, law firms must be able to retrieve their data and backups must be retained for agreed periods. After agreed periods, the CSP must permanently delete the data. This is necessary both to mitigate the risk of loss of confidentiality and for compliance with the PDPA which requires that personal data is not held for any longer than is necessary. A reputable CSP will use best practice procedures and a data-wiping solution which are compliant with the National Institute of Standards and Technology's Guidelines for Media Sanitization.

Compliance

Managing compliance is a complex task that is difficult for an organization to navigate on its own, even more so for regulated industries. Not only are there numerous standards and regulations, these are constantly changing making it even more difficult for a business to keep abreast. In today's complex regulatory environment, law firms should identify the well-established security and privacy certifications that are important to their organisations and require that their CSPs demonstrate to their conformance to those. This plays a vital role in providing assurance of conformance with expected norms for security and privacy. In addition, greater weight should be given to a CSP who commits contractually to routinely undergo validation by independent third party auditors, as having an independent and qualified third party certify compliance is a stronger form of attestation. Other certifications which may not be specifically relevant can be indicative of industry best practice and can also be taken into consideration.

Law firms are advised to ask the CSPs to share details of their independent certifications, and are advised to look for cloud service providers that conform to ISO/IEC 27001 and ISO/IEC 27018 (an important cloud computing standard for the protection of personal data in a public cloud). In addition to international security standards, law firms can also check if the CSP is certified against MTCS SS584. This is a Singapore-issued system of certification for cloud services providers, with different tiers applying to different categories of data depending on its business criticality. The MTCS SS584 was launched by the Information

Development Authority of Singapore, and was announced to be compulsory for participation in Singapore government bulk tender.

Transparency

This is the foundation for any trusted CSP. Lawyers need both choice and visibility into the cloud practices of the CSP – including where their data is stored, who can access it and under what circumstances. Therefore, they must choose a CSP that provides complete clarity to the marketplace regarding its cloud practices. There should be clearly stated and readily available policies and procedures so that law firms can understand as much as possible about how that data is handled. These details can be part of the contract service agreements, backed up by third party audit reports and certifications.

1. A CSP ought to provide transparency in the following areas:
2. Cloud contract terms that are clear and understandable;
3. Identification of subcontractors used to deliver cloud services;
4. Easy access to third party audit reports;
5. Periodic reports detailing law enforcement requests for data; and
6. Location of data at rest.
7. Managing the Cloud Contract

Beyond signature of the contract, law firms must continue to be vigilant and have appropriate oversight of the CSP throughout the contract lifecycle. Law firms can obtain assurance that the CSP meets the necessary regulatory requirements on an ongoing basis by reviewing information provided by the CSP, including the audit results arising from contractually required independent third party assessments.

In addition, the decision to use CSPs does not relieve law firms of the responsibility to ensure data is protected. For example, while CSPs should provide security for certain elements through the design and configuration of their cloud services (such as the physical infrastructure and network elements), the law firm must also be aware of its own responsibilities in protecting the security and privacy of its clients' data.[7] Law firms should have an information security policy with employees embracing a data privacy first and data security first mindset. Training should also focus on cybersecurity awareness, effective password hygiene, utilizing multi-factor authentication practices and identifying social engineering and phishing schemes.

Conclusion

Cloud computing will continue to gain traction for the legal industry. Law firms must identify the challenges and mitigation strategies arising from the transfer of responsibility over sensitive data and applications to a CSP. A suggested framework for such risk evaluation is based on four key principles of trust: security, privacy and control, compliance, and transparency. Some of the challenges can be addressed by contract and "must-have" provisions include: detailed data protection terms; meaningful service level obligations; prompt security incident notification; clarity on third party access to data; no use of data by a CSP for advertising or similar commercial purposes; customer ownership of data; data location specificity; independent verification of key commitments; and CSP responsibility for third party sub-contractors.

Jennifer Koo is currently the lead attorney for Microsoft Singapore. In this role, Jennifer is responsible for the company's corporate, external and legal affairs in Singapore. This includes supporting commercial transactions and providing regulatory counsel to business groups on public policy issues such as intellectual property rights, privacy and internet security and safety. Before joining Microsoft, Jennifer was with eBay as its legal counsel responsible for Southeast Asia. Jennifer started her career in Rajah & Tann, focusing on intellectual property technology, entertainment and communications law. Jennifer is a co-founder of womenLEAP, a group for legal, executive and advisory professionals to connect, collaborate and network and she is passionate about women in leadership.

Notes

1 How the Cloud is positively transforming the Legal Sector, 23 June 2017, Computer Business Review <http://www.cbronline.com/news/cloud/cloud-positively-transforming-legal-sector/>

2 Comment on Rule 1.1 of the American Bar Association Model Rules of Professional Conduct <https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html>

3 The Law Society of Singapore Guidance Note on Cloud Computing provides a good summary of the deployment models and service delivery models.

4 Guidance Note on Government Cloud First Policy <https://www.gov.uk/guidance/government-cloud-first-policy>

5 Rule 35(4) Professional Conduct Rules and the Law Society of Singapore Guidance Note on Cloud Computing

6 See for example, Wee Shou Woon v HT SRL [2017] SGCA 23.

7 The Law Society of Singapore Guidance Note on Cloud Computing.