FINANCIER WORLDWIDE corporatefinanceintelligence

HUNTON& WILLIAMS

Outsourcing to the cloud: data security and privacy risks

BY PETER BRUDENALL, BRIDGET TREACY AND PURDEY CASTLE

A recent innovation in outsourcing has been the use of 'cloud computing' technologies. Major IT vendors, such as Microsoft and IBM, now routinely incorporate cloud computing architecture within their service offerings. Customers are attracted by the advantages of on-demand access to services, the ability to leverage economies of scale, a broad geographic distribution of services, and the ability to flex services to meet fluctuating levels of demand. The advent of cloud-based platforms is revolutionising data storage and processing. However, as data moves away from an organisation's protected infrastructure, ensuring data security and compliance with data protection laws will become even more of a challenge.

What is the cloud?

Cloud computing is emerging as a component of IT outsourcing that enables vendors to offer traditional IT facilities through the cloud on a more flexible basis than may be possible with traditional, fixed infrastructure-based services. The term 'cloud computing' has defied precise description by industry experts. Recently, the US National Institute of Standards and Technology defined cloud computing as a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources….that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Cloud-based services may utilise a variety of models. For example, organisations may employ private clouds, community clouds, public clouds or hybrid clouds. Outsourcing using a non-private cloud, a key feature of which is the pooling of resources to serve many customers simultaneously, shares many of the risks of traditional outsourcing arrangements. These risks are difficult to mitigate through contract negotiation as there is limited opportunity to customise the service delivery. However, as with a traditional outsourcing model, these risks may be managed through effective due diligence and the active management of the vendor relationship.

Key considerations when outsourcing to the cloud

Know your data. Storing data with a cloud provider may trigger additional domestic and foreign legal obligations. Under EU data protection law, individuals have a right to access, block or delete their personal data. Where employee data is stored in the cloud, employee works councils will require assurances that these rights of access will be guaranteed. They will also seek assurances that data security will not be compromised. Works councils will resist new technologies that may compromise employees' rights or put employees' data at risk, and may even seek to block the implementation of such technologies. It is crucial, when planning an outsourcing project, that an organisation undertakes due diligence on its own data to establish exactly what data will be hosted in the cloud, to what extent such data consist of sensitive, confidential or business critical data and to determine what the organisation is entitled to do with that data (including considering whether there are any constraints on transferring the data to third parties or abroad). Works councils must be engaged early. A failure to address these issues at the outset can result in added costs and increased risk to the business.

Vetting the vendor. It is essential that data security and data protection considerations feature in the initial vendor due diligence. Surprisingly, organisations are sometimes unaware of the fact that cloud technology is used by their vendors to deliver outsourced services. The large multinational vendors, which provide an array of sophisticated cloud-based services, are more likely to be proactive in ensuring data security and facilitating the data protection compliance obligations of their customers than the smaller, national vendors. As in a traditional outsourcing arrangement, organisations should carefully analyse the vendor's solution to determine whether cloud-based technology is used and to ensure that additional regulatory compliance issues are addressed. This initial due diligence should then be supplemented by the exercise of audit rights during the life of the outsourcing arrangement.

Data security. Data security issues are a key consideration in any outsourcing arrangement, irrespective of whether data are held in the cloud. Under EU data protection laws, organisations remain responsible for the personal data of their customers and employees and must guarantee its security even when a third-party processes the data on their behalf. Therefore, if a cloud vendor suffered an intrusion or security breach, European data protection enforcement action would focus on the organisations using the cloud, not on the cloud vendor. This is a very significant issue for businesses in Europe, which are increasingly nervous of the reputational (and financial) impact of data breach.

Data transfer. Cloud models contemplate data being transferred across multiple locations and may result in an inability to identify the precise location of the data within the cloud at any point in time. EU data protection laws impose restrictions on the international transfer of personal data outside of the EEA unless certain conditions are satisfied. Such conditions are often burdensome and impractical in the context of the cloud but unless organisations place restrictions on which locations their data may be transferred to, organisations may be exposed to a myriad of regulatory regimes without their actual knowledge. In response to these concerns, some cloud vendors offer EU-based services.

Service levels. A risk with all new technology is the possibility of downtime and data being unavailable. Some cloud vendors are currently unwilling to provide any level of guarantee around service availability – a significant concern for any company dependent on access to its data. Negotiating appropriate service levels, as well as conducting due diligence on the cloud vendor's technical infrastructure, will be essential to gaining confidence that the vendor has the ability to ensure appropriate access to, and availability of, data.

Going forward

Cloud computing provides organisations with an alternative to tradi- ▸▸

This article first appeared in Financier Worldwide's *March 2010 Issue.*

tional outsourcing arrangements, often with significant cost benefits. We can expect the technology to continue to develop and adapt to suit changing demand. As organisations seek new ways to achieve efficiencies, more organisations may choose to outsource using cloud based technology. The extent to which organisations will enter into cloud-enabled outsourcing arrangements will, in part, depend upon cloud vendors' ability to address organisations' data security and privacy concerns.

As the model matures, there are some practical steps that organisations may take to manage cloud-based risks: (i) consider whether a cloud-based outsourcing model is appropriate or permitted given the type of data involved; (ii) undertake appropriate due diligence paying particular attention to the safeguards the cloud vendor deploys to protect customer data; (iii) understand the data flows and identify applicable domestic and foreign laws that may affect whether and, if so, how data may be processed in the cloud; (iv) negotiate a robust contract, which imposes best practice security standards (including access controls) on the cloud vendor and grants wide rights of audit; (v) encrypt data prior to sending it to the cloud and require the cloud vendor to use encryption technology; (vi) seek to control the locations to which the data are transferred and retain visibility of any subcontracting arrangements; and (vii) ensure data are backed up outside the cloud and that the cloud vendor has appropriate disaster recovery and business continuity arrangement. ■

Peter Brudenall and Bridget Treacy are partners and Purdey Castle is an associate at Hunton & Williams. Mr Brudenall can be contacted on +44 (0)20 7220 5700 or by email: pbrudenall@hunton.com.

Peter Brudenall
Partner
T: +44 (0)20 7220 5725
E: pbrudenall@hunton.com
www.hunton.com

Peter Brudenall is a partner in the firm's Global Technology, Outsourcing & Privacy Group.

Peter has extensive experience in advising companies on technology procurement and major outsourcing projects, with a particular focus on acting on offshore outsourcing arrangements. He also advises companies on technology contract disputes, cloud computing arrangements, software development and licensing, and the exploitation of intellectual property.

Bridget Treacy
Partner
T: +44 (0) 20 7220 5731
E: btreacy@hunton.com
www.hunton.com

Bridget Treacy is a partner in the firm's Global Technology, Outsourcing & Privacy Group.

Bridget's practice focuses on complex technology transactions, including outsourcing and IT procurement. In addition, Bridget has market-leading experience of data privacy issues, particularly in the context of implementing outsourced arrangements. Increasingly, these projects rely on cloud computing architectures, raising particular data protection and information security issues. Bridget has advised cloud vendors and cloud users on these issues.

Purdey Castle
Associate
T: +44 (0) 20 7220 5723
E: pcastle@hunton.com
www.hunton.com

Purdey Castle is an associate in the firm's Global Technology, Outsourcing & Privacy Group.

Purdey's practice focuses on complex technology transactions including information technology and business process outsourcing and transactions involving the procurement, distribution and licensing of technology products and services. Purdey also advises on all aspects of technology law, with emphasis on electronic commerce, data protection and information security.