Does the cloud put data sovereignty compliance out of reach?

A look at the complex issue of data sovereignty as enterprises begin to embrace SaaS technologies.

Data sovereignty. A decade ago, these two words together would have resulted in many blank stares in the majority of boardrooms. Today, speak these two words to Fortune 500 CIOs and CISOs, and they will most likely end up with their head in their hands. Data sovereignty is a critical emerging topic. It addresses the legal and regulatory jurisdictions governing particular digital information and how vendors, customers, and users can manage these overlapping jurisdictions.

What's changed? Why has this topic become such a hotbed for IT professionals, compliance officers, and corporate boards around the world? The cloud happened, and the overwhelming majority of corporate content is now digital and networked. Removed from the physical constraints of hard copy, networked digital documents can be copied and moved between locations or jurisdictions with negligible effort. For cloud-based services, defining data 'location' is complex. Information is distributed across multiple physical, logical, and legal locations. As the potential benefits are widely publicized and frequently achievable, the modern enterprise continues to move towards cloud-based solutions. Most managers and directors are peripherally aware and mindful of the significant consequences, damage to professional reputation, and financial losses if their use of cloud technologies goes wrong. However, they pass over dealing with these risks with the "probably won't happen to me" mentality or they simply overlook them for the sake of efficiency.

The intended audience for this paper is anyone involved with corporate operations looking to use SaaS applications and cloud data storage; legal departments, finance, risk managers, IT professionals, and corporate executives are all interested parties. Its intent is to provide an understanding of the complexities data sovereignty brings to the use of cloud-based services.

Why are data sovereignty and jurisdiction important?

Regulators and courts around the world have begun to focus on the entire stores of information held by corporations and how they manage this information. Each time a new story of a security breach at their favorite blue-chip brand company makes the evening news, the general public is reminded about the vulnerability of the information in the cloud. Governments increasingly require transparency for specific types of data and these national institutions – whether legislatures, courts, law enforcement, regulators, or NGOs – are increasingly sensitive to the implications of distributed data:

- How can the privacy of a citizen's information be protected when it is stored outside of the country? With a foreign-based vendor?
- How can regulators ensure that they have access to sensitive information (e.g. financial information, drug trial data) stored outside the regulating country?
- How can I ensure that I am compliant with data privacy rules set forth by the European Union member countries?
- How can national courts retain jurisdiction over enforcement of national laws for cloud-hosted data?

Taking the corporate risk perspective, businesses need to carefully examine the implications of moving data to the cloud. Laws in other countries may be different than the one in which your business entity exists. If your business operates internationally, be aware that governments typically have a much easier time getting access to your data if it is within their jurisdiction. As such, be sure to examine the legal mechanisms that any given country may have put in place to allow third-party access to your data, such as subpoenas, national security letters, mutual legal assistance treaties, etc. Lastly, the topics of data sovereignty and information security have increased professional liability for companies. The inability to protect data from unwanted demands of third parties creates risks with large financial penalties as well as damage to the personal reputation of the executives of the company in question.

Productivity & innovation vs. security & risk

Because most cloud/SaaS vendors continue to be US-based, the impact of data sovereignty concerns is being felt most acutely by companies doing business in Europe and Asia – particularly in highly regulated industries. Facing a complex regulatory environment, these companies either limit adoption of cloud/SaaS technologies or accept regulatory risk from non-compliant solutions. According to Gartner research vice president Carsten Casper, "Business leaders must make the decision and accept the residual risk, balancing different types of risk: ongoing legal uncertainty, fines or public outrage, employee dissatisfaction, losing market share due to a lack of innovation, or overspending on redundant or outdated IT."[1]

Businesses must balance the flexibility and potential cost savings of the cloud with the risks inherent of storing data beyond the company's direct control … and determine how that risk is amplified if the data is stored in a foreign country.

1. http://www.gartner.com/newsroom/id/2787417

CIOs need to engage their company's IT, security, and legal departments when evaluating cloud vendors. They need insight into potential vendors' security programs including who can access data, technical aspects of the infrastructure, and the location of the data.

Finding balance

For global enterprises, there is no single solution to the challenge of data sovereignty regulation. Instead, companies must take a holistic enterprise approach when evaluating cloud technologies. As mentioned earlier in this paper, the vetting of a particular cloud service provider must be done cross functionally to include the legal, risk management, and security views of the organization; it should not be a decision left solely to IT or the line of business. Does the vendor align itself with common international standards such as ISO 27001? Does it have a record of reliability? What methods does it use to prevent unauthorized access to data? These questions are just the start of what should be a thorough examination.

Next, companies should plan to carefully review and negotiate the contract with a service provider. Many solutions that began as consumer-oriented services often use simple contracts that may not have the necessary detail to protect the business.

Finally, global enterprises should look to match their defined information governance rules and processes to technology capabilities that fit the varying requirements of the industries in which they compete and in the countries they do business. Specifically they should look to enable:

- **Separation of data control from physical location:** By separating physical storage from the logical control point of information, businesses can benefit from the cloud and distributed data while still maintaining ultimate control over their high-risk information.

- **Control of data location:** Where data residency is required for regulatory compliance, businesses must be able to control where their cdata is stored and processed.

- **Content as the new security perimeter:** Regardless of where data is stored and processed, the greatest risk to information comes when it is in use – which often crosses both corporate boundaries and national borders. The solution is information rights management to protect and track specific information, wherever it is shared.

- **Discipline and transparency:** For third-party cloud vendors to be trusted by national institutions, they not only need best-practice security technology and processes, but they also must be able to prove themselves trustworthy.