IDG CONNECT

IDG CONNECT

Research Paper

DATA SOVEREIGNTY

The Cloud, despite its aura of intangibility, is still a physical server hosted somewhere. But now that companies' data is being stored outside the safety of the physical organization, often on a server unknown, the rules have changed. With expert commentary, this paper analyses the level of knowledge and fear surrounding Data Sovereignty in the IT community.

June 2013

Master Of Your Cloud? The Data Sovereignty Survey

When Obama signed an extension to the Patriot Act, something interesting happened. People became worried the US would be able to access their data, no matter which country they resided in, because it was kept on the Cloud. When questioned, Microsoft couldn't promise that people's data was secure on their Office 365 Cloud service, because though you may be working from the EU, Microsoft is a US company and has to comply with the rules, and doesn't necessarily have to tell you about it. These rules apply to Gmail, Amazon and a host of others, despite various EU laws aimed at preventing this kind of situation, because they are all US companies.

When all this information came to the fore, it put the spotlight on two things; the Big Brother-esque approach the US seems to be taking, and the issue of Data Sovereignty. Though the Act is the main culprit of Data Sovereignty hysteria, it's just the tip of the Cloudy iceberg.

The legal term is 'trans-border data flow'. Each country has their own data laws, all varying in strength and in regard to issues such as privacy and security, which is fine when you know where that data is being stored and are familiar with those rules. But Cloud computing is changing the traditional models. IDC predicts that in 2013, worldwide IT spending will exceed $2.1 trillion - with Cloud computing being one of the main drivers. In mature markets, public Clouds are expected to rise in popularity - Gartner predicts 60% of companies in the US increasing their public Cloud in the year to come. But how much understanding is there on these services? Do organizations know where their Cloud is hosted, and more importantly, who has legal access to it in that country? To gauge awareness of Data Sovereignty and concerns surrounding the issue, we surveyed 217 business & IT professionals from 42 countries.

Summary

- 70% of organizations are concerned about Data Sovereignty
- But just 36% are aware of relevant laws & legislation

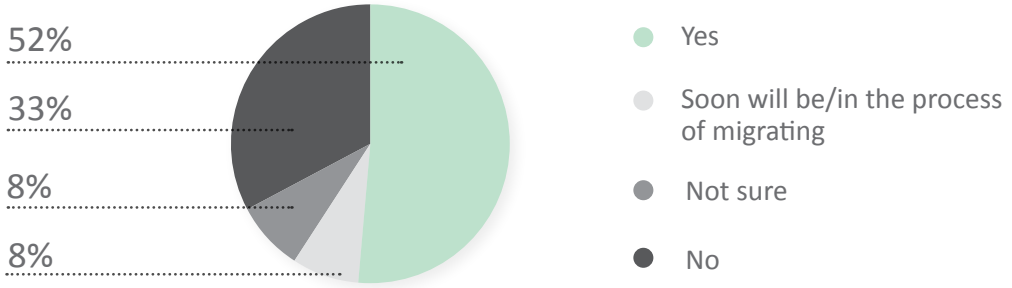
Of companies that use the Cloud:

- 23% know which country their Cloud is based and relevant data laws

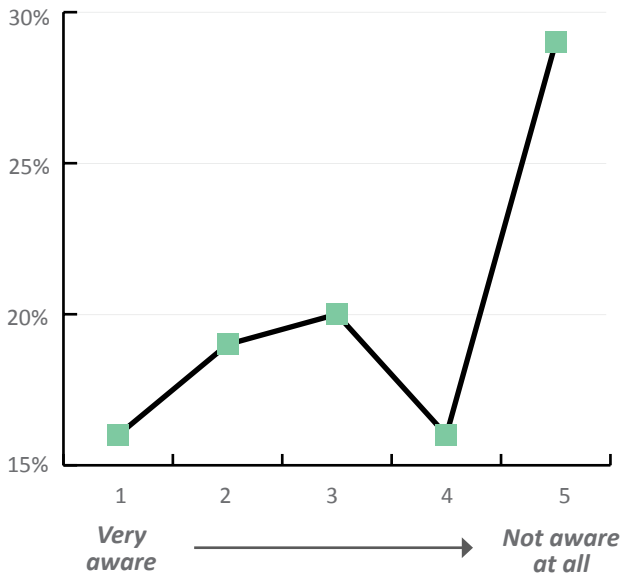
Of companies currently migrating to the Cloud:

- Just under 50% know where their Cloud will be stored - but all of those know the local data laws

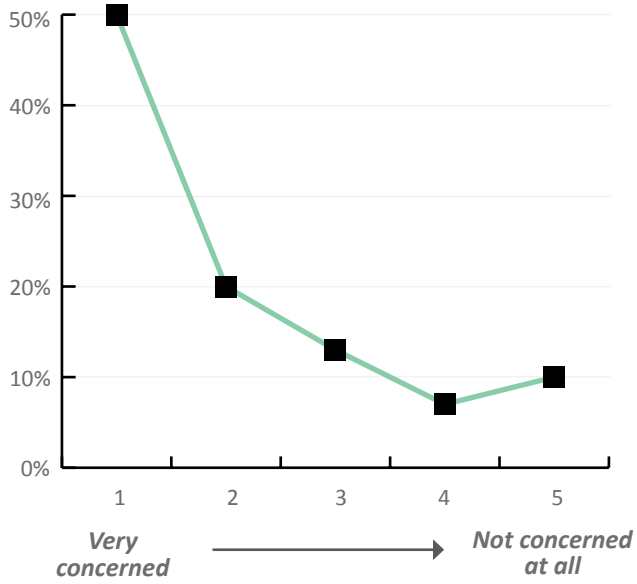
Do you save data on the Cloud?



How aware are you of Data Sovereignty laws and issues?



How worried are you about Data Sovereignty issues?



Findings

The main lesson learned from our survey is that Data Sovereignty is a major concern for companies, but only a minority have any substantial knowledge on the issue. 70% of companies rated themselves as concerned on the matter, but just over a third are aware of the relevant legislation. The awareness of the rules seems to be closely tied to usage and knowledge of the Cloud, but the worry is universal. There seemed to be no regional trends on awareness or concern.

The majority (60%) of companies in the survey either currently or soon will be using the Cloud. Of those, just a quarter of companies who do use or will soon be using the Cloud know where that data is being stored and know the relevant data laws for that country. 100% of those companies who know where their Cloud is are aware of Data Sovereignty laws. Concern among those with knowledge on their Cloud's location was high, irrelevant if they knew the local data laws.

23% of people who use the Cloud know where their Cloud is, and the relevant data laws.

Just under 50% of those soon migrating know where their Cloud will be stored - compared to a third of those already on the Cloud. Almost 100% of those migrating companies know the relevant data laws, compared to around half of those already in the Cloud. Those in the process but unsure about where their data is being stored generally had vague awareness of Data Sovereignty laws & issues, and their levels of concern were generally lower too.

100% of those who know where their Cloud currently is are aware of DS laws

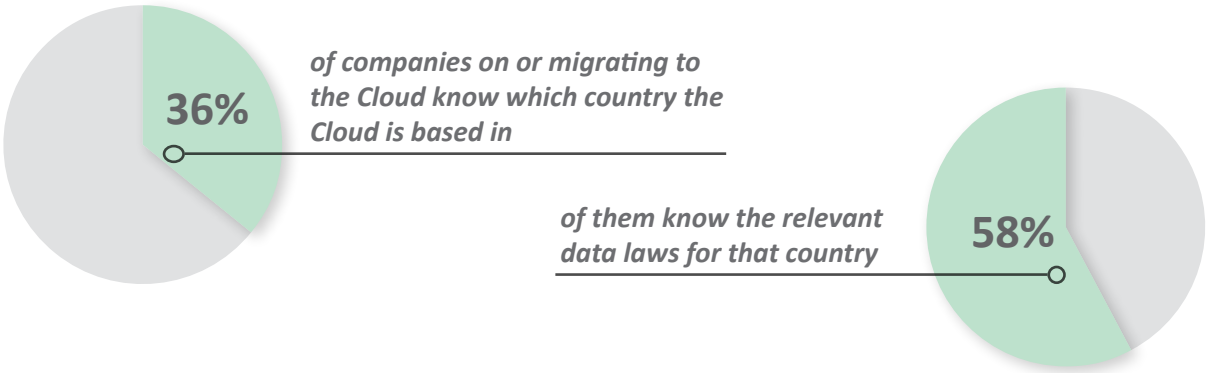
63% of companies on the Cloud do not know where their Cloud-based data is held, and their awareness of Data Sovereignty laws & issues were also low - half had no knowledge on the subject - but concern was still high.

Non-Cloud Users

Around a third of companies are not yet using the Cloud and not currently making plans to. Their awareness on the subject of Data Sovereignty varied, as was their levels of concern. But greater awareness leads to greater levels of concern.

Unsures

8% of respondents were unsure if they were on the Cloud or not - understandably their awareness of Data Sovereignty was low, but around half rated themselves concerned on the issue



Background

With Obama's signing of the Patriot Act Extension and the subsequent lack of reassurance from Microsoft and others over the safety of Cloud data, no matter where it was stored, the Cloud stopped being a magical thing. The fact that the Cloud was really a physical data center hosted somewhere else finally hit home.

Where that physical manifestation of the Cloud was based was suddenly important, because if it's outside your normal jurisdiction, whose rules should it follow? The Patriot Act might have been the start, but Data Sovereignty is a far bigger set of rules.

Pirate Bay's journeyman approach to data hosting has highlighted how sketchy laws can be when it comes to data. Though recently the company is having domain troubles having switched from Swedish to Greenland-based domains, the Privateers moved to the Cloud in order to escape being shut down. Even before the Cloud, the company had been linked to countries that exist outside regular jurisdiction, such as sea fort-turned-Micronation, Sealand, and North Korea.

Recently, UK PM David Cameron had to sign a cybersecurity pact with the Indian government after deciding to host government data in the country, in order to reassure those concerned that this wasn't a fool-hardy idea. As Ian Lamont, IT security specialist at BMW told GigaOM; a stock photograph from a brochure might be ok to store anywhere, but "customer data or the company's crown jewels? No way." Adding to the problem is a lack of information and involvement on where the data is stored. "It doesn't help for a bank to hear its customer data will be in this European cloud 'region'. Not specific enough."

So while most won't mind the US to looking at their Facebook pics and inane Tweets, people may not be so keen on the idea of them getting a hold of bank details, or private messages. Likewise, with governments increasingly turning to the Cloud, the stakes become even higher - another country being able to access your whole identity is kind of scary, no?

People may argue that as long as you stay on the legal side of things everything is hunky dory, but that's an opinion, not a guarantee. It's also worth noting that the Patriot Act, while being the media grabber, isn't the only law of this kind and lots of countries can get their mitts on Cloud data, that doesn't make it any more ok, does it?

Ignorance is Bliss

Despite the PR hype the Cloud has had, there's still a degree of misunderstanding around it. According to Citrix, a worryingly large segment (22%) of people think Cloud computing has something to do with the weather. Knowledge around Data Sovereignty is even patchier, and while white papers do exist, but lack of awareness is still a danger.

Currently, if you want to try and protect your data and embrace all those Cloud benefits, there are few options really. Keep data in-house, and be very cautious about where your data goes and make sure you know all the details when it is being stored elsewhere. For Cloud service providers, being open about where the data is being held, and what assurances they can provide on its protection should come as standard.

50% of those who don't know where their Cloud is are unaware of Data Sovereignty

While new rules governing certain areas, for example more pan-EU legislation on the issue, isn't out of the question, that only fixes the problem to a certain extent. Cloud computing is a global concept, one which needs a globally unified set of rules that everyone can play along to. As long as the rules vary by state, region, island, etc., the paranoia over who owns what, who's snooping where, and which country Pirate Bay will be based in next, will never end.

Expert Opinion: George Gardiner, *Gardiner & Co.*

Many organisations are playing fast and loose by taking a laissez-faire attitude to Data Sovereignty in the Cloud, argues George Gardiner, a London-based lawyer specialising in the ICT sector who is currently drafting a paper on the topic.

"Disaster recovery and business continuity issues are no different to having data stored locally because you can still do backup even in the Cloud," he says. "But access to the data is often the issue because how do you physically get to data if the supplier goes into liquidation or there's a failure in the service? Anybody who hasn't addressed what is nothing more than a well known continuity issue is asking for trouble."

Larger and more sophisticated buyers are increasingly electing to specify that data does not travel beyond the EU when negotiating with Cloud service providers in order to comply with legal and regulatory requirements; aside from avoid shareholders' wrath and reputational damage. This has clear benefits but does not constitute optimal governance, however.

"Where the data resides is a crucial issue and if it is within the EU then that's certainly a tick in one box but that doesn't mean your service provider has in fact complied with the Eight Principles of the EU Directive, particularly in respect of security. You cannot take a company on its paper assurances that it is meeting all the legal and regulatory requirements - there ought to be independent third-party confirmation of this (taking into account the nature of the data and the value of it or the harm which would be caused by its loss or disclosure)."

That's where internationally recognised data security comes into play. However, there is no concrete assurance that the data won't end up outside of Europe. "If, for example, the US government requires a large US company to provide access to data outside of the USA, such as in a Dublin data centre, what are the chances of that large company ignoring the US government?"

There are always risks. Unless data centres are competently managed, there is no certainty that an automated management routine such as load balancing will not send data over to a foreign datacentre. Also, Gardiner has no truck with the suggestion that data perceived as low-value or not sensitive will be an exception and can therefore travel wherever in the world.

"Data protection law ignores the perceived commercial value of the data. The data must have some commercial value, which needs to be safeguarded, otherwise why would a business go to the expense of using it within the Cloud," he says.

Buyers of Cloud services also need to be familiar with the small print. For example, on some platforms data might be encrypted in data stores but not over networks, thus incurring the risk of interception. And where data is encrypted, do you trust the holder of the encryption keys? Again, verbal and even contractual assurances may be comforting but do not absolve a business from establishing the level of security in the first place. While a business may have complied with the law, this will not necessarily protect it from reputational harm if there is a massive data leak.

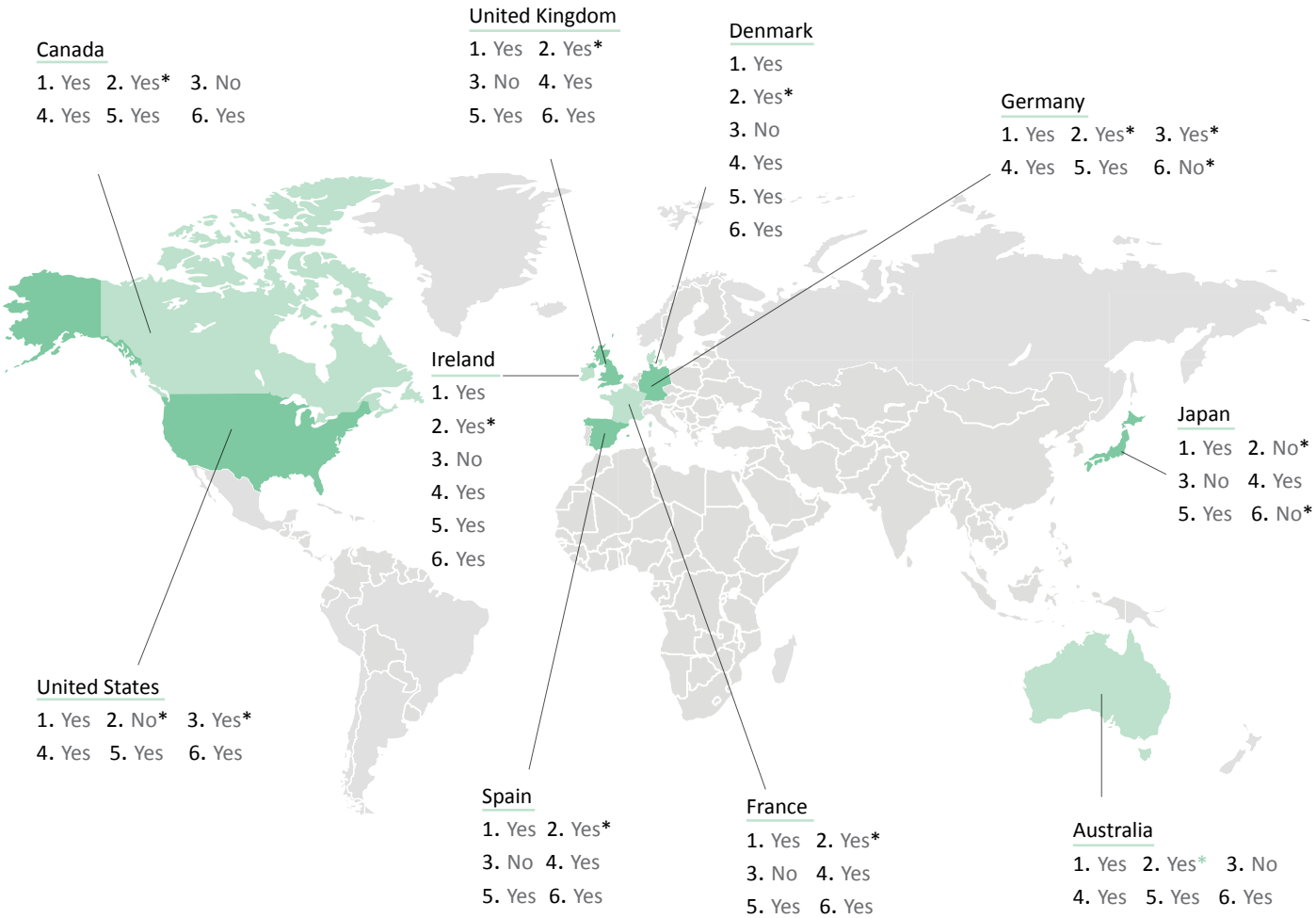
Over the last few years companies "have wised up" to these vagaries, Gardiner says, but growing penalties, such as the Information Commissioner being able to fine companies up to 5% of their global turnover, mean buyers must be aware of all risks.

"The middle players [among businesses using Cloud services] aren't aware of those risks or don't have the competency to deal with them," Gardiner warns. "It might be naivety but that's no defence under the law. All too often I come up against techies who want to do something that's easy to do but introduces significant regulatory and legal risks. Just because it is possible doesn't mean it is a good idea."

Governmental Authorities' Access to Data in the Cloud: A Comparison

Legend:

1	2	3	4	5	6
May government require a Cloud provider to disclose customer data in the course of a government investigation?	May a Cloud provider voluntarily disclose customer data to the governament in response to an informal request?	If a Cloud provider must disclose customer data to the government, must the customer be notified?	May government monitor electronic communications sent throught the systems of a Cloud provider?	Are government orders to disclose customer data subject to review by a judge?	If a Cloud provider stores data on servers in another country, can the government require the Cloud provider to access and disclose the data?



* with exceptions

[Source: Hogan Lovells "A Global Reality: Government Acces to Data in the Cloud"]

Conclusion

Our findings show that while concern over Data Sovereignty is high, actual working knowledge on the subject remains low - with only a small minority fully educated in both the location of their data and its safety. Those moving to the Cloud now have a greater awareness of where their data will be stored and the relevant local data laws, even if their awareness of the wider Data Sovereignty issues remains average.

About IDG Connect

IDG Connect, a division of International Data Group (IDG), the world's largest technology media company, produces, publishes and distributes local IT and business information on behalf of a truly global client base. Established in 2005, we have a fully nurtured audience of 2.6 million professional decision-makers from 130 countries, and an extended reach of 38 million names. This lets us conduct research, create independent analysis and opinion articles, and drive long-term engagement between professionals and B2B marketers worldwide. For more information visit www.idgconnect.com