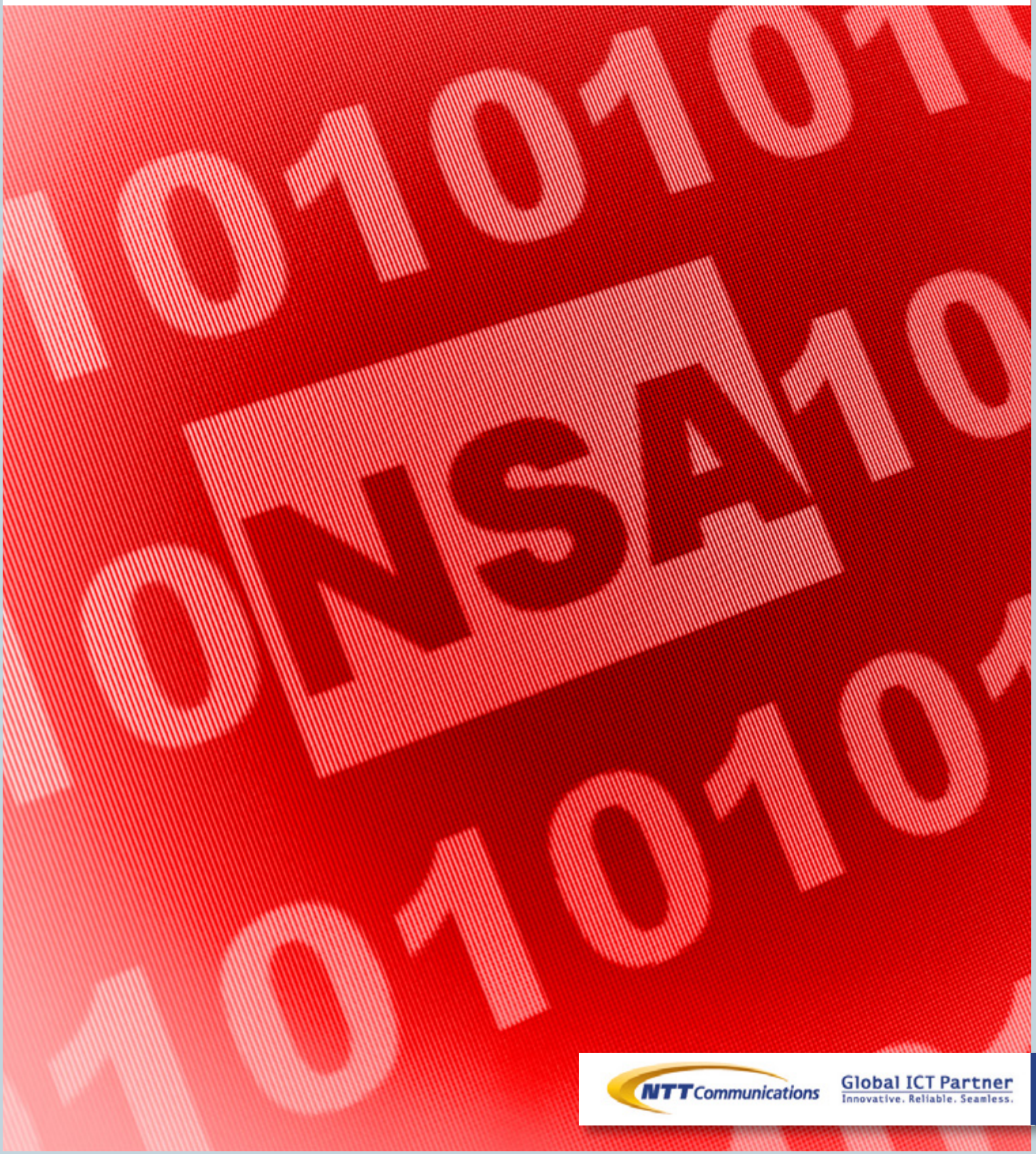
NSA After-shocks

How Snowden has changed ICT decision-makers' approach to the Cloud



NTT Communications

Global ICT Partner
Innovative. Reliable. Seamless.

FOREWORD

2013 was a game-changing year for cloud service providers across the globe. Edward Snowden's revelations of covert data gathering and cyber-surveillance programmes carried out by the National Security Agency (NSA), the UK's GCHQ and other intelligence services, rocked public trust in the Internet. The revelations have hit many of the world's largest technology companies hard: Google, Apple and Microsoft have together called on the US government to rein in their surveillance activities.

Businesses are also concerned and they are acting decisively to protect their data by keeping it where they know it will be safe. This is the key finding of a study of ICT decision-makers in large companies in France, Germany, Hong Kong, the USA and United Kingdom, that we completed at the beginning of March 2014, and whose findings are summarised here.

This report paints a picture of ICT decision-makers who wish to protect their company's data even if it means delaying cloud computing projects that could deliver them much-needed flexibility and performance gains.

The report does make it clear that ICT decision-makers really want the best of both worlds. They want to guarantee the sovereignty of their data ***and*** reap the benefits of cloud computing. But they can only do so if they can specify exactly where and how their data is stored in the cloud.

NTT Communications can give customers this capability, thanks to its global team of more than150 data centers, and a low-latency network that touches almost 200 countries.

We hope you enjoy reading this paper and find the action points we set out at the end valuable. Our team would be happy to discuss any questions or observations you may have.

NTT Communications

info@ntt.eu

For any media enquiries please contact Brands2Life on:

NTTComms@brands2life.com

+44 20 7592 1200

EXECUTIVE SUMMARY

The world of corporate ICT has been rocked by Edward Snowden's revelations of large-scale cyber-surveillance by US and other governments. These leaks from June 2013 have had a direct impact on how companies around the world think about ICT and cloud computing in particular. And the revelations may not have ended according to the TED talk[1] published during the creation of this report.

NTT Communications' survey of 1,000 ICT decision-makers in France, Germany, Hong Kong, the United Kingdom and the USA has found:

- **After-shock 1:** Almost nine in ten (88 percent) ICT decision-makers are changing their cloud buying behaviour, with over one in three (38 percent) amending their procurement conditions for cloud providers
- **After-shock 2**: Only 5 percent of respondents believe location does not matter at all when it comes to storing company data
- **After-shock 3:** More than three in ten (31 percent) ICT decision-makers are moving data to locations where the business knows it will be safe
- **After-shock 4:** Around six in ten (62 percent) of those not currently using cloud feel the revelations have prevented them from moving their ICT into the cloud
- **After-shock 5:** ICT decision-makers now prefer buying a cloud service which is located in their own region, especially EU respondents (97 percent) and US respondents (92 percent)
- **After-shock 6**: Just over half (52 percent) are carrying out greater due diligence on cloud providers than ever before
- **After-shock 7**: One in six (16 percent) is delaying or cancelling contracts with cloud service providers
- **After-shock 8**: More than four fifths (84 percent) feel they need more training on data protection laws
- **After-shock 9**: 82 percent of all ICT decision-makers globally agree with proposals by Angela Merkel for separating data networks

The content of the study paints a vivid picture of real concern for the sanctity of corporate data in the cloud. A further key finding is that ICT decision-makers still very much value the cloud as a platform for boosting business agility and technology innovation, so even though there is disquiet, there is also optimism that the industry will address these concerns. ICT decision-makers need a way to retain the benefits derived from cloud computing whilst protecting the organisation, and the data it holds, from being compromised in any way. To that end, we conclude this report with some actionable guidance points which we would recommend to any ICT professional concerned over their organisation's exposure to cyber-surveillance.

HOW THE RESEARCH WAS CARRIED OUT

NTT Communications commissioned market research firm Vanson Bourne to carry out an extensive independent survey of 1,000 ICT decision-makers from France (200 respondents), Germany (200 respondents), Hong Kong (100 respondents), the UK (200 respondents), and the USA (300 respondents), in February and March 2014. Sixty percent of respondents were drawn from businesses with 1,000 employees or more, representing sectors including financial services, retail, manufacturing, professional services, ICT, and energy.

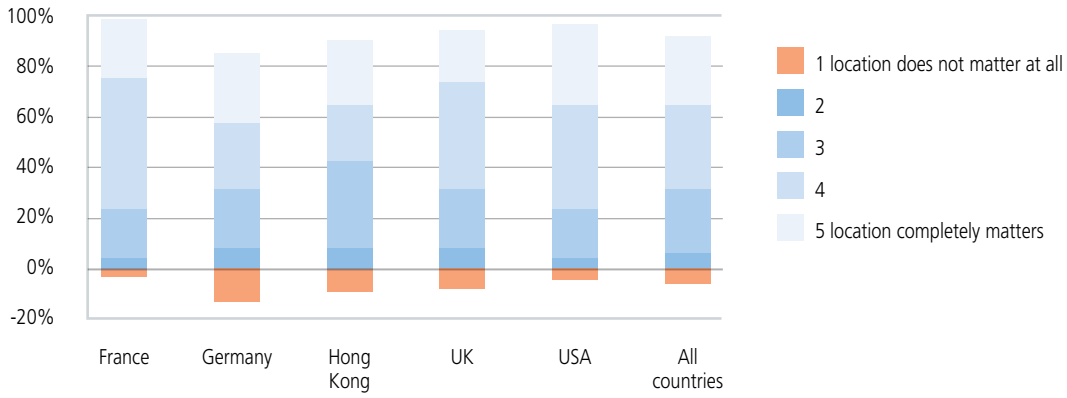
[1] TED Talk – TED 2014
http://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet

WHERE'S MY DATA? SOVEREIGNTY MATTERS TO ICT DECISION-MAKERS IN THE POST-SNOWDEN WORLD

The physical and virtual worlds are uneasy bedfellows when it comes to business data, and NTT Communications' survey of ICT decision-makers finds them landing decisively on the side of the physical world. Only 5% of respondents believed that the location of business data was unimportant.

Moreover, almost one third (30 percent) of ICT decision-makers in Germany and the US agreed that 'location completely matters' when thinking about data storage in the cloud. In France and Hong Kong, almost a quarter (24 percent), and in the UK, about a fifth (22 percent), held this view (chart 1).

Chart 1: To what extent does geographical location matter in regard to where your company data is stored?



A substantial proportion of respondents are acting decisively on their concerns. Across the five countries surveyed, almost a third of ICT decision-makers (31 percent) said they are moving their business data to where they know it will be safe. Our study finds Germany leading the way, with 40 percent of respondents there holding this view, followed by France (37 percent), Hong Kong (31 percent), and then the USA (29 percent). Only a fifth of ICT decision-makers in the UK (18 percent) agreed.

What does a 'safe place' look like to ICT decision-makers? Respondents from all five countries surveyed overwhelmingly preferred to procure cloud services from within their own continents. In the UK, France and Germany the same proportion of respondents – 97 percent – said they would prefer to contract with European cloud providers. 92 percent of US ICT decision-makers held the same view – this time with regard to US providers. In Hong Kong, the figure is markedly lower – just 69 percent said they would prefer to work with Asia-Pacific providers. Interestingly, 39 percent also said they would contract with European providers – perhaps a reflection of the close commercial ties between Hong Kong and Europe (chart 2).

Chart 2: From which region would you feel most comfortable buying a cloud service offering?
(Respondents from each region specifying their home continent)

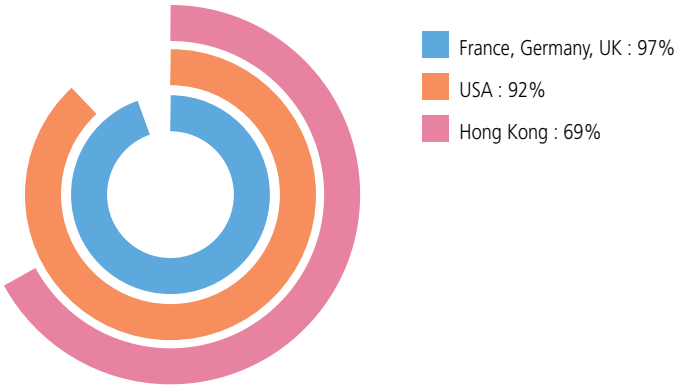


Chart 3 provides a different view of ICT decision-makers' thinking. When asked whether they would purchase cloud solutions from providers that are either headquartered in another country, or whose data centers are abroad, the view is far from unanimous.

Around one in five of all respondents stated they would not buy cloud solutions from foreign providers, or from those whose data centers were abroad.

Keeping data in their own country was most important to German ICT decision-makers (32 percent of respondents agreeing), followed by the UK (24 percent) and France (23 percent). By contrast, only 16 percent of US respondents, and 17 percent in Hong Kong took the same view.

The nationality of providers was another consideration. Again, almost a third of German ICT decision-makers said they would not purchase cloud solutions from providers headquartered abroad, followed by France (24 percent). But in the UK, the USA and Hong Kong, concern over the nationality of providers was less significant. Just 16 percent of ICT decision-makers in the UK, and 14 percent in the USA and Hong Kong, viewed this as a problem. By contrast, 33 percent of respondents in the US clearly have a concern over the revelations as they would definitely buy cloud services from providers headquartered abroad, as did a quarter of respondents in France and Hong Kong (19 percent in both the UK and Germany).

Chart 3: Cloud provider locations matter
(all respondents in all countries)

It is clear that, in the post-Snowden world, keeping data close to the business, and mapping it to a suitable global network and data center footprint, has become a crucial first step for organisations considering a move to the cloud. Indeed, ICT decision-makers across the world are subjecting cloud providers to broader scrutiny, as the next section explains.

SNOWDEN COMPELS CLOUD BUYERS TO LOOK BEFORE THEY LEAP

Aside from the critical issue of the location of data, the study has also uncovered evidence that ICT decision-makers are scrutinising cloud providers more closely before signing up. This has come as a direct result of the allegations of NSA surveillance, of which almost every respondent worldwide had some knowledge (chart 4).

87 percent of the ICT decision-makers polled agreed that the Snowden allegations have changed their approach to cloud computing to some extent.

A significant proportion of the ICT decision-makers polled said they are postponing or shelving cloud projects altogether. One in six respondents (16 percent) said they are delaying or cancelling projects. This view was most widely held in Hong Kong (23 percent of respondents), followed by the US and Germany (19 percent) and France (15 percent). In the UK, just 6 percent of respondents held this view.

Chart 4: Are you aware of the recent allegations of foreign surveillance by the NSA and similar authorities?

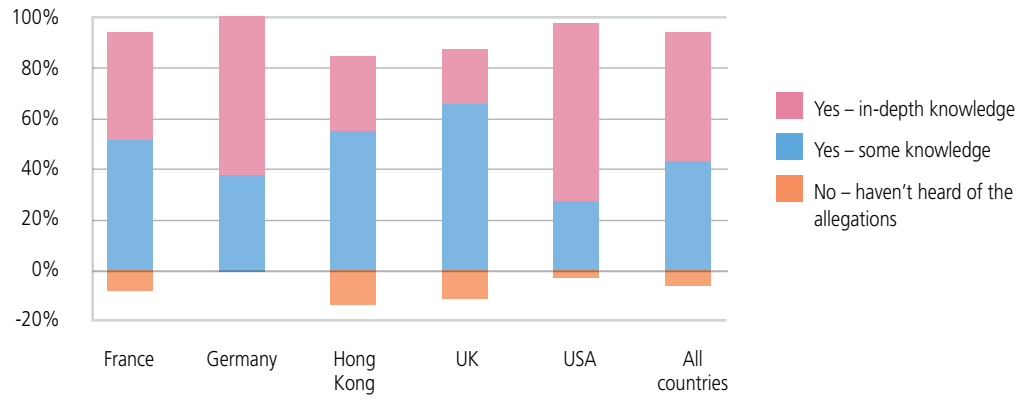
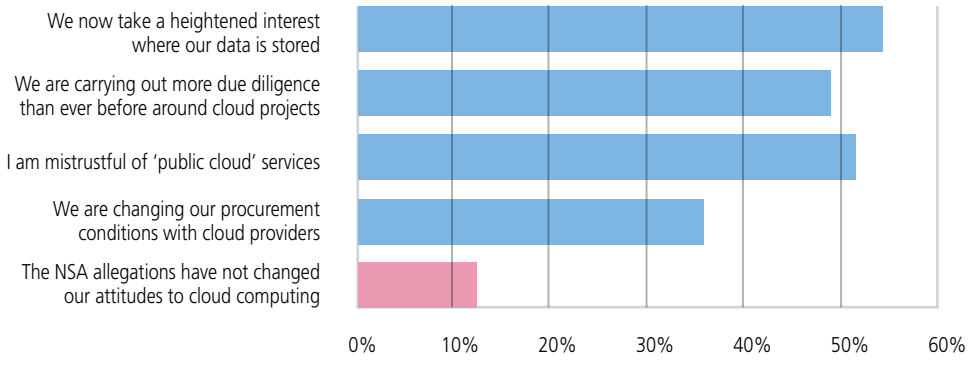


Chart 5: Snowden revelations harden attitudes to the cloud
(all countries, those agreeing or agreeing strongly with each statement)



The findings paint a picture of ICT decision-makers who are anxious to ensure the integrity of their data and are scrutinising their providers in that regard. They are also examining their own capabilities to make sure they can mitigate risks to their business. In particular, they are focusing on security, legal scrutiny, and training.

The following sections explore these measures in greater detail.

THE STATE OF CLOUD ADOPTION WORLDWIDE

Cloud adoption is strong across the board with 88 percent of ICT decision-makers using the technology within their business, either as private or public cloud. Of those surveyed, the French and US have the highest usage of cloud compared with the rest of the world. Over two thirds (71 percent) of French businesses are using private cloud with less than half (42 percent) using public cloud. The US is ahead with 82 percent of ICT decision-makers using private cloud and over half (56 percent) using public cloud.

When looking into the length of time that cloud has been used within a business, it found that over half (51 percent) of ICT decisions-makers across the world have been using cloud for two years or more. France was the most cloud-friendly nation surveyed with two thirds (61 percent) of businesses using it for more than two years.

Average cloud usage 2+ years (51 percent):

- France – 61 percent
- Germany – 39 percent
- Hong Kong – 46 percent
- UK – 46 percent
- USA – 58 percent

A. MORE RESOURCES FOCUSED ON SECURITY

Following what the business community has learned about online surveillance, organisations are planning to invest more in data security. Two thirds of respondents (67 percent) agreed they have audited their cloud suppliers' security credentials rising to four in five (83 percent) of ICT decision-makers in the USA. In France and Germany, almost 70 percent had carried out an audit, while in Hong Kong 58 percent of respondents, and in the UK, 47 percent had carried out an audit. It is not clear from the survey whether budgets have been reallocated from other areas, perhaps affecting other projects, or whether they have been increased absolutely; others may care to investigate this.

Almost four respondents in five (76 percent) said they have been forced, to some extent, to change how they manage their cloud security budgets. While the vast majority of respondents agreed that extra investment would go towards added security measures, training was also seen as a key priority. Nearly two thirds (65 percent) of ICT decision-makers in the USA and Germany said they plan to invest more in training, followed by France and Hong Kong (60 percent and 58 percent respectively). In the UK, the figure was 47 percent.

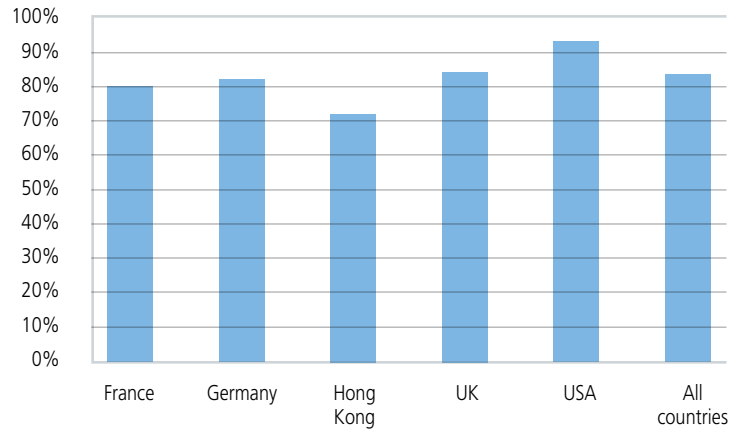
B. COLLABORATION BETWEEN ICT AND LAWYERS INCREASES

Our survey has found that the ICT department is taking an increasing interest in compliance initiatives in the wake of the Snowden revelations.

Nearly three quarters (72 percent) of ICT decision-makers polled said they would revisit every cloud and hosting arrangement to ensure data protection, if they had the necessary time and resources. Almost nine in ten (86 percent) of US respondents held this view, as did three quarters (75 percent) of French respondents. German, UK and Hong Kong respondents agreed but less so (65 percent, 62 percent, and 62 percent respectively).

The Snowden revelations have also made ICT decision-makers more aware of the need to have detailed knowledge of data protection rules. 84 percent of ICT decision-makers globally believed they need training on data protection laws and security rules in the territories their businesses operate (chart 6).

Chart 6: I believe ICT decision-makers need training in understanding data protection laws and regulations (those agreeing or strongly agreeing)



The study suggests that respondents still view cloud providers as a potential source of valuable compliance expertise. 81 percent of ICT decision-makers said they would prefer to partner with providers who understand differing security and data protection requirements in each country. US and UK respondents felt strongest in this regard (89 percent and 87 percent respectively), followed by France (75 percent), Germany (73 percent), and Hong Kong (72 percent).

C. TRAINING – THE PEOPLE SIDE OF CLOUD

ICT decision-makers' keenness to partner with cloud providers on these issues may be symptomatic of the wider skills shortage affecting the cloud computing sector. Industry analyst IDC reported that 1.7m cloud computing jobs globally could not be filled because candidates lacked the necessary training and experience needed to work in cloud-enabled businesses[2].

According to our findings, the Snowden revelations have thrown the staff training issue into sharp relief. Three quarters (75 percent) of ICT decision-makers want to educate staff on security and compliance in the workplace. Concern over this issue is most pronounced in the USA, where 88 percent of respondents agreed, followed by Germany (77 percent), France (75 percent), the UK (62 percent) and Hong Kong (60 percent). Sixty percent of respondents are investing more money in this area.

[2] IDC report published in November 2012 – Climate Change: Cloud's Impact on IT Organisations and Staffing

POLICY IMPLICATIONS: RETREAT OR ENCRYPTION?

The Snowden revelations brought about discussions at Government levels addressing the possibility of ring-fencing country communications, so that data would fall under national regulations.

These plans were taken one step further by German Chancellor Angela Merkel, who in February 2014 made a call for European internet services to be entirely separated from the USA. She said: "we'll talk with European providers that offer security for our citizens, so that one shouldn't have to send emails and other information across the Atlantic."[3]

Though many industry figures see these proposals as near-impossible to put into practice, they have promoted discussion of alternative approaches to safeguarding private data in the cloud. **82 percent of ICT decision-makers questioned as part of this study are aware and agree with proposals by Angela Merkel for the creation of European data networks.**

In particular, the wider use of encryption has emerged as a more feasible counter-measure to cyber-surveillance. Senior ICT executives discussed this very topic at a round-table debate hosted by NTT Communications at Cloud Expo Europe 2014, in London.

The participants agreed that, while currently-available encryption technology could indeed provide the means to protect data both in transit and in storage in the cloud, operational issues and its performance overheads would render it difficult to implement widely – at least in the short term.

Nevertheless, all speakers agreed that – thanks to the Snowden revelations – encryption is now being discussed more than ever. One of the round-table participants, Ilja Summala, CTO of Nordcloud, said "The revelations of cyber-surveillance have made companies more conscious of placing sensitive data in the cloud. Even though buying decisions have not necessarily changed as yet, encryption has been pushed to the top of the corporate agenda. There is a big opportunity for those that can provide easy encryption at all levels."

[3] Financial Times, 16th February 2014
http://www.ft.com/cms/s/0/dbf0081e-9704-11e3-809f-00144feab7de.html

CONCLUSION: A SAFE AND SECURE CLOUD?

Does this mean ICT decision-makers have given up altogether on the cloud as a delivery platform for enterprise ICT? The survey suggests not: three out of the five countries covered by the study – and 71 percent of the respondents overall – believed their data would be safer in some form of cloud platform, subject to guarantees over data integrity (chart 7).

In spite of the Snowden revelations, it is clear that ICT decision-makers all over the world still subscribe to the idea that the cloud provides the most cost-effective means to scale and deliver increasingly sophisticated ICT services to business users.

What appears to have changed, though, is the nature of the cloud customer. ICT decision-makers have been quick to learn from the current crisis and now understand how to scrutinise providers. Those suppliers that can live up to the increased demands for data integrity, governance and security will find success in the post-Snowden world.

Chart 7: Please rank the following options in order of where you believe your data would be safest, where 1 is safest, and 5 is least safe

(Combination grid showing the percentage of respondents who ranked each option either first, second or third)

	France	Germany	Hong Kong	UK	USA	All countries
With a cloud provider who can provide guarantees over the physical location of data	79%	73%	63%	65%	72%	71%
On your own hardware in your own IT facilities	59%	77%	66%	86%	64%	70%
A cloud run by a company with a reputation for trustworthiness	60%	67%	70%	55%	70%	64%
On your own hardware in a shared datacentre (colocation)	47%	52%	49%	66%	44%	51%
A cloud provider with a global footprint and local offices	57%	33%	52%	29%	49%	44%

TAKING ACTION

Recommendations from NTT Communications for those cloud buyers that are concerned about their cloud supplier:

1. Seek assurances over the physical location of data – the right providers will be able to provide undertakings over sovereignty
2. Ensure your providers allow you to restrict, move, or definitively destroy data
3. Scrutinise cloud providers' ownership and business structure
4. Examine security credentials and certifications
5. Talk to the supplier's customers if you can, particularly those that are subject to compliance regimes similar to your own

Footnote from NTT Communications - *We take our clients' data protection very seriously and constantly enforce all appropriate measures to comply with all applicable laws and jurisdictions in the countries that we operate. If government, police, legal or security organisations request access to data, systems, logs, or other customer specific information then we will expect a court order, warrant, subpoena or other appropriate legal document enforcing access.*

NTT Communications Corporation

1-1-6 Uchisaiwai-cho
Chiyoda-ku
Tokyo 100-8019
Japan

www.ntt.com

Contact Us: info@ntt.eu

Connect with us:

NSAAS032014-1