The DATA CENTER Journal

Where IT, Facilities and Design Meet

Volume 33 | August 2014

IT Security in a Post-Snowden World:

Dealing With Data Sovereignty and Data Custody Issues

Designing Reliable Physical Security for the Data Center

For daily data center news and information visit www.datacenterjournal.com

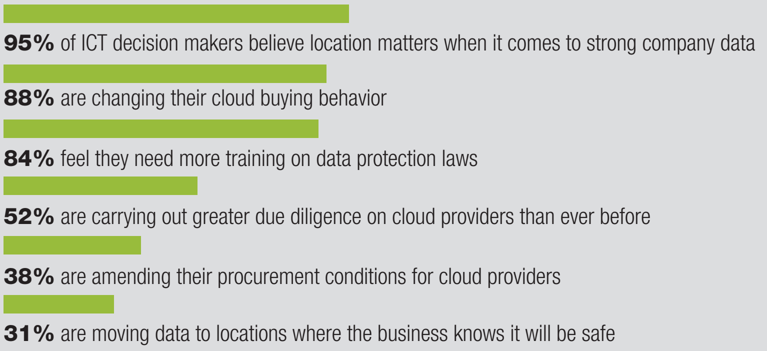
FEATURE

IT Security in a Post-Snowden World:

Dealing With Data Sovereignty and Data Custody Issues

BY BOB BUTLER

Have the Snowden Revelations Changed Your Approach to the Cloud?



95% of ICT decision makers believe location matters when it comes to strong company data

88% are changing their cloud buying behavior

84% feel they need more training on data protection laws

52% are carrying out greater due diligence on cloud providers than ever before

38% are amending their procurement conditions for cloud providers

31% are moving data to locations where the business knows it will be safe

Source: NTT Communications, March 2014

I’ve been working in or around IT security for more than three decades, and I can’t remember the last time that a cyber-security issue received such sustained attention from the public media. It has been over a year since former NSA contractor Edward Snowden released a trove of documents revealing the large-scale collection, analysis and storage of personally identifiable information—much of it from the data centers of telecommunications, Internet and cloud service providers. And people are still talking about it.

But conversations about data sovereignty and data custody—re-ignited by Snowden’s revelations—are not only important to private citizens. They pose, as you’ll learn in this article, significant challenges for the enterprise as well. So to the question of the current state of IT security and next steps, addressing the issues of data sovereignty and data custody is essential.

IT INFRASTRUCTURE DECISION MAKING IN A POST-SNOWDEN WORLD

The Snowden revelations are not the only factor making data sovereignty and data custody challenging issues for the enterprise. Another significant factor is the coincident proliferation of global IT infrastructure options and the rising ubiquity of the cloud. There’s no question that this proliferation of options is key to our ability to manage the ever-increasing amount of data we generate and consume. But all these options, and the global nature of them, make IT management much more complicated than it was in that not-too-distant past.

When your IT infrastructure is located on your premises or colocated with a data center provider, there’s no question where your data is. You have the key to the cabinet; the answer to the question “Who has custody?” is easy—it’s you. But when your data applications or infrastructure—even some of them—are in the typical public cloud, it can be difficult or impossible to say where in the world your data resides, much less where it has been. (That is data sovereignty.) The amount of control you have over your data depends on the laws of the country where it is and the policies of the cloud service provider. (That is data custody.)

Enterprise leaders overwhelmingly understand the importance of location when it comes to storing company data, and many have taken or are planning new action to protect the privacy and security of their data. Yet the fact remains that data sovereignty and data custody present legitimate challenges for global enterprises. And those challenges are not going away.

THE ISSUES: DATA SOVEREIGNTY AND DATA CUSTODY

Data sovereignty is the question of which sovereign’s (i.e., country’s) laws govern your data. The concept is often taken to mean that your data is subject to the laws of the country in which it is located, but that may not be the case; data sovereignty may instead mean that the data is subject to the laws of the country in which it originated, or the laws of the country in which the cloud provider is headquartered. In the cloud, data sovereignty can become an issue because different countries have different laws governing the collection, use, storage and transmission of data within their borders.

Sometimes the laws that apply are less “friendly” than your own sovereign’s laws, putting enterprise data and customer data at risk. In other cases, the laws are significantly more strict, requiring levels of privacy protection, for example, that your cloud provider may not be equipped to accommodate.

Navigating these different (and sometimes conflicting) laws can be quite difficult. It depends on knowing—and controlling—where your data is. If you don’t know where the servers that hold your data are, you don’t know whose rules you might be beholden to. And if you don’t know (or can’t control) whose rules you might be beholden to, you can’t know whether the jurisdictional laws in that location are in sync with your corporate policies and your sovereign’s data laws.

In fact, many of the benefits of the cloud are based on the premise that data is moved swiftly between data centers as cloud providers distribute workloads in order to optimize the capacity and efficiency of their servers, and to create better resiliency for business continuity of operations. Yet “the ease with which cloud resources can be allocated and reallocated makes it more likely that it will be done without an appropriate review of the relevant legal issues.”[1]

[1] QMUL Cloud Computing Project, “What

Issue	Business Decision	Solutions
Are the jurisdictional laws in the given location in sync with your corporate policies and your sovereign's data laws? (Typically applies when the laws are "less friendly" than your own sovereign's laws, potentially putting enterprise data and customer data at risk.)	If the answer to that question is no, you may not want IT infrastructure in that location, or you may want to operate under tighter control with more robust security than you might otherwise deploy.	On-premises or off-premises (a.k.a., any-premises) private cloud *and* End-to-end encryption to secure the data in transit
Is your cloud provider capable of accommodating the laws of the countries in which you do business? (Typically applies when the location's laws are stricter than your own sovereign's laws, requiring higher levels of privacy protection, for example.)	If the answer to that question is no, and you want to do business in that given location, you'll have to figure out how to comply with local laws.	Colocation in a local data center *or* Any-premises private cloud
Do any of the locations in which you do business require you to keep their citizens' data in-country?	If the answer to that question is yes, and you want to do business in that given location, you have to figure out a way to keep the data in-country.	Colocation in a local data center *or* Any-premises private cloud
Are you prepared to protect enterprise data and government data even in the face of surveillance programs that you're not aware of?	Without knowledge of the programs the government is running, it's impossible to make informed business decisions. So in the face of potential secret programs, preemptive measures may be necessary.	Any-premises private cloud *and* End-to-end encryption to secure the data in transit
Do you know, and are you comfortable with, what your cloud provider would do if the government of any of the countries in which your enterprise data is running or stored asked it to turn over your data or your encryption keys?	There are many reasons an enterprise would decide to go to the public cloud. But there are risks that must be accounted for and mitigated; most public cloud providers do not provide the level of visibility and control that most enterprises require.	Public cloud *and* Rigorous due diligence *and* You control the encryption keys *or* Any-premises private cloud

A Framework for IT Infrastructure Decision Making in the Context of Data Sovereignty and Data Custody Issues

WHAT HAPPENS HERE STAYS HERE?

Partly in response to Snowden's revelations, countries including many in Europe and Asia as well as Australia, New Zealand and Brazil are focused on passing laws that require that data generated within their borders stay within their borders. Why? Because when the data of one country's citizens leaves its borders, the country loses the ability to regulate the use of that data. And many countries are increasingly concerned that data privacy laws in other countries—like the U.S.—don't offer the kind of protections their citizens expect or national leadership desire.

For many enterprises, the cloud is a way to have a data center "presence" everywhere they do business. But if data generated in one country of the many you do business in is required to stay in that country, will your cloud provider be willing—or able—to abide? When the answer is no, some suggest that the enterprise seek a local cloud provider. But due diligence can be difficult from across the ocean, and the capabilities and data custody practices of nascent cloud providers—especially in emerging markets like Asia and Latin America—are not yet clear.

Beyond geographic location, who is managing the infrastructure that stores your data and runs your applications certainly matters because you have outsourced performance, security and governance to that provider. But it also matters from a data custody perspective. To put it bluntly, if a government comes knocking with a subpoena, will the service provider hand over the keys?

IT INFRASTRUCTURE SOLUTIONS TO ADDRESS DATA SOVEREIGNTY AND DATA CUSTODY ISSUES

Addressing critical data sovereignty and data custody issues is about making fully informed business decisions: Decisions about which locations you want IT infrastructure in, and which you don't. About which infrastructure model best suits both your needs and the data sovereignty and data custody particulars of the location. About what kinds of security processes and due-diligence procedures should be put in place.

The table provides a framework for the sorts of business decisions an enterprise will face with each data sovereignty and data custody issue, along with the solutions that the enterprise should consider.

A GLOBAL IT INFRASTRUCTURE PLATFORM PLUS VISIBILITY AND CONTROL

In considering the range of available IT infrastructure solutions to address data sovereignty and data custody issues, it becomes clear that the enterprise IT infrastructure model of the future is one in which decisions are made based on a wide range of factors, including data sovereignty and data custody decisions.

The risk with that kind of fit-for-purpose, locate-anywhere model is that enterprise IT infrastructure becomes a patchwork of siloed, non-interoperable resources. Some custom-built, one-off data centers of different vintages, colocation through different providers around the world, cloud services from a range of vendors.

That kind of IT infrastructure patchwork compromises the enterprise's ability to securely and efficiently achieve business and performance objectives. Guarding against it requires an IT infrastructure platform that enables the enterprise to make infrastructure decisions that are optimized around each geography's data sovereignty and data custody particulars—using a combination of the solutions described above as it makes the most sense in each location. When that best-fit IT infrastructure is part of a platform, it's globally interoperable.

Critical to the platform, and to all of the solutions listed above, is the ability to see and control where data is running and where it is stored—and who has access to it—at every location. That visibility and control is essential for the enterprise to be able to make fully informed decisions. And it requires a data center operating system (DCOS). Sometimes referred to as being the same as data center infrastructure management (DCIM), a true data center operating system actually goes far beyond monitoring and reporting of data center assets to include control and automation. A single, global data center operating system enables visibility into and control over all IT infrastructure around the world.

According to 451 Research, data center operating systems "can provide real-time 'live' information by constantly checking operational data. They can (usually) also detect and provide immediate notification of problems such as equipment failures, hotspots or issues with power distribution. Alarms and data about separate events can be correlated so managers can readily determine the root cause(s) and which equipment has been affected."[2]

THE BOTTOM LINE

Data sovereignty—where your data resides—does matter. Data custody—who controls your data—is critical. Addressing those issues is about making fully informed business decisions: Decisions about which locations you want IT infrastructure in, and which you don't. About which infrastructure model best suits both your needs and the data sovereignty and data custody particulars of the location. About what kinds of security processes and due-diligence procedures to put in place.

With full visibility and control into where your data is and who has access to it, you can confidently make the best IT infrastructure decisions for the business—in today's post-Snowden world, and beyond. ■

About the Author: Bob Butler is the chief security officer at IO, a worldwide leader in software-defined data center technology, services and solutions that enable businesses and governments to intelligently control their information. Before assuming his current role at IO, Bob served as the first Deputy Assistant Secretary of Defense for Cyber Policy. To learn more about how IO helps organizations resolve data sovereignty and data custody issues, visit io.com.

is Cloud Computing?" Queen Mary University London, 2010.

[2] 451 Research, "Prefabricated Modular Datacenters: 2014 and Beyond," Dec 2013.