DARK SKIES AHEAD

Just as cloud was beginning to gain acceptance in the Middle East, concerns over data security came to a head this year as news of the PRISM surveillance programme broke. Can the big cloud vendors work around this, or is there a gloomy outlook for cloud in the region?

And it was all going so well. As vendors began to build more comprehensive cloud-based product roadmaps, Middle Eastern users were beginning to see just how cloud services can streamline their businesses. According to a Gartner report from earlier in the year, cloud adoption was due to grow monumentally in the region up to 2016. This was largely due to issues surrounding security and compliance being ironed out.

It'd be easy to say that the rest is history, but earlier this year, an NSA contractor called Edward Snowden leaked documents suggesting the existence of a blanket digital surveillance programme known as PRISM. The documents inferred that the US government had access to any file hosted by the country's big tech vendors — including the ones that provide cloud services to millions around the globe. Suddenly, vendors' assertions that your cloud data will always be secure seemed much less sincere.

According to Natalya Kaspersky, CEO, InfoWatch, businesses need to take these news developments seriously, even if they're not even adopting a cloud strategy.

"If we talk about Google Docs, for example, now we clearly understand that Google shares information of its clients with the USA National Security Agency.

> **"If you don't use Google Cloud, you'd probably use Google Search or maybe Facebook, Microsoft Office or other computer tools developed in the USA. That means, one way or another, you will be under Big Brother's eye."**
>
> Natalya Kaspersky, CEO, InfoWatch

This causes concerns, so if you don't use Google Cloud, you'd probably use Google Search or maybe Facebook, Microsoft Office or other computer tools developed in the USA. That means, one way or another, you will be under Big Brother's eye. This is the reality that companies need to understand," she says.

For those looking to adopt a cloud strategy, the allegations over NSA spying are much more pertinent. It speaks volumes that, when we contacted the big American vendors about this article, the question on whether regional customers are now wary of US-based cloud services was dodged in more than one case.

But according to Jatin Sahni, Vice President, Large Enterprise and Business Solutions Marketing, du,

Middle Eastern businesses definitely are wary about US-sourced cloud services. "It is a key question that is driving a lot of the decisions to adopt cloud services from American companies or cloud services storing data in American data centres," he says.

This is good news for a local telco such as du, as regional operators have begun to offer world-class cloud services to rival the American ones. Now that the PRISM news has broken, the likes of du and Etisalat have enticed users with assertions that data is hosted locally — not in the US where the NSA might have access to it.

"More advanced services, such as hybrid clouds, PaaS and niche applications platforms, are being developed and offered locally, and would put local

> "More advanced services, such as hybrid clouds, PaaS and niche applications platforms, are being developed and offered locally, and would put local providers on par with international offerings."

Jatin Sahni, Vice President, Large Enterprise and Business Solutions Marketing, du

providers on par with international offerings," Sahni says.

Even the big, American corporations have to admit that local cloud service providers look a little more attractive these days. But according to Ahmad Muammar, Systems Engineer Manager, Gulf, EMC, this isn't just down to concerns over privacy. What's more, larger customers might still want to go for the bigger providers.

"I believe that local service providers, or global ones with a strong local presence, are the ones who will win more business in the enterprise sector, and this is not specific only to the Middle East," he says. "For SMBs, the market will split between local CSPs who are more attractive due to data privacy and regulations, and others who will go to global providers who give them a cost advantage due to the scale of economy."

Cost isn't the only advantage that comes from dealing with a large cloud provider, according to Louay Dahmash, Head of Middle East, Autodesk. He believes that companies looking to pursue a cloud strategy should be more concerned about technical knowhow than data privacy. Sure, the NSA might potentially have access to your data, but — as we wrote earlier this year

> "Businesses in the Middle East realise that, to reap the benefits of cloud technologies, it is important to work with providers with a high level of sophistication and knowhow with regards to the technology."

Louay Dahmash, Head of Middle East, Autodesk

HOW TO SECURE YOUR CLOUD DATA

Sudheer Subramanian, Senior IT Solutions Manager, Huawei Enterprise Middle East

Security and privacy of data is the number-one priority for all businesses when moving to the cloud. The challenge facing IT managers today is how to realise the benefits of cloud while maintaining control over the data and ensuring the organisation is protected from damaging data breaches.

A few tips to consider in order to ensure that your data is safe:

1) **Secure your data transfer:** Make sure your data is always travelling through a secure channel; only connect your browser to the provider via a URL that begins with 'https://'.

2) **Secure your software interface:** Customers should be aware of software interfaces, or APIs, that are used to interact with cloud services. Reliance on a weak set of interfaces and APIs exposes organisations to a variety of security issues related to confidentiality, integrity, availability, and accountability.

3) **Secure your stored data:** Data should be encrypted to ensure that it is secured in the service provider's storage system.

4) **Separate your data from others:** Should a customer wish to migrate their data to a cloud service provider, they should ensure that their data is not exposed to other customers who may have their application hosted in the same environment. A multi-tenant DC environment, for instance, should ensure that data is compartmentalised and encrypted, so that there is minimal risk of unauthorised data access.

— that shouldn't be an issue if you have nothing to hide.

"Businesses in the Middle East realise that, to reap the benefits of cloud technologies, it is important to work with providers with a high level of sophistication and knowhow with regards to the technology," he says. "Local controversies will have a short-term impact on businesses, but eventually, for the benefit of the customer, businesses will have to partner with the best, some of which are organisations from mature economies."

Kaspersky, a big advocate of data privacy, admits that "the Middle East isn't a leader in software development, so Gulf companies need to use solutions from international vendors."

What's more, Kaspersky believes that cloud computing will still continue to be adopted more widely, simply because businesses can save on costs using it. Indeed, there's no doubting that cloud services make up a compelling prospect to the average SMB owner, says Rajesh Abrahim, Director of Product Development, eHosting DataFort.

"Not many enterprises bought into the idea straight away but the hype is now turning into reality and we are seeing increased uptake. We see a higher uptake for non-critical workloads and more and more small businesses adopting the public cloud because of benefits such as access to latest technology, monthly subscription fees and low total cost of ownership," he says.

EMC's Muammar says that businesses shouldn't look at cloud differently because of the PRISM allegations. Instead, they should be looking at how the cloud can help them cut costs and become more agile. If businesses align their cloud strategies to their business objectives, the prospect of adopting cloud becomes too good to ignore, he believes.

"Cloud can be seen as the efficiency frontier — one which can add a lot of agility to the organisation's foundation of execution. Cloud will continue to

> **"I believe that local service providers or global ones with a strong local presence are the ones who will win more business in the enterprise sector, and this is not specific only to the Middle East."**
>
> Ahmad Muammar, Systems Engineer Manager, Gulf, EMC

Until 2016, the UAE cloud market is set for a compound annual growth rate of

43.7%

be one of the biggest drivers of IT and business transformation, helping enterprises achieve efficiencies that were not possible earlier. As we go further in this journey, there is no doubt that we will see more and more organisations revamp their strategies to continue to align IT objectives to larger business goals to further drive growth and competitive differentiation," he says.

The numbers are on Muammar's side. In a recent survey conducted by IDC, over 80 percent of high-level IT decision makers in the region's financial sector — a vertical traditionally opposed to cloud computing — acknowledge that cloud computing offers significant benefits. And according to the research house, the UAE cloud market alone is set for a compound annual growth rate of 43.7 percent until 2016.

This might be great news, but what about the privacy risks now associated with cloud? What's more, were the previous issues around security and compliance really ironed out before the NSA leaks? According to Kaspersky, there are still problems that need addressing, but there are solutions, too.

"Service providers don't take the legal responsibilities for client's data in the cloud. But as soon as the clients put their data in the cloud they essentially lose control over the information. It's extremely hard to provide a legal environment for using data in the cloud since service providers give no guarantees that client's data won't leak. Therefore, securing a client's data through insurance companies can be one of the proposed solutions, which still hasn't been implemented so far," she says.

Whether it is worth taking that risk now is up to CIOs themselves. Some have adopted cloud strategies simply because of the benefits it can bring their businesses — and they've done it using big, American tech vendors. Others may want to be more cautious. One thing is for sure, though — with the controversy surrounding PRISM continuing to rage, coming up with a good cloud strategy just got that much harder. ■

> **"We see a higher uptake for non-critical workloads and more and more small businesses adopting the public cloud because of benefits such as access to latest technology, monthly subscription fees and low total cost of ownership."**
>
> Rajesh Abrahim, Director of Product Development, eHosting DataFort