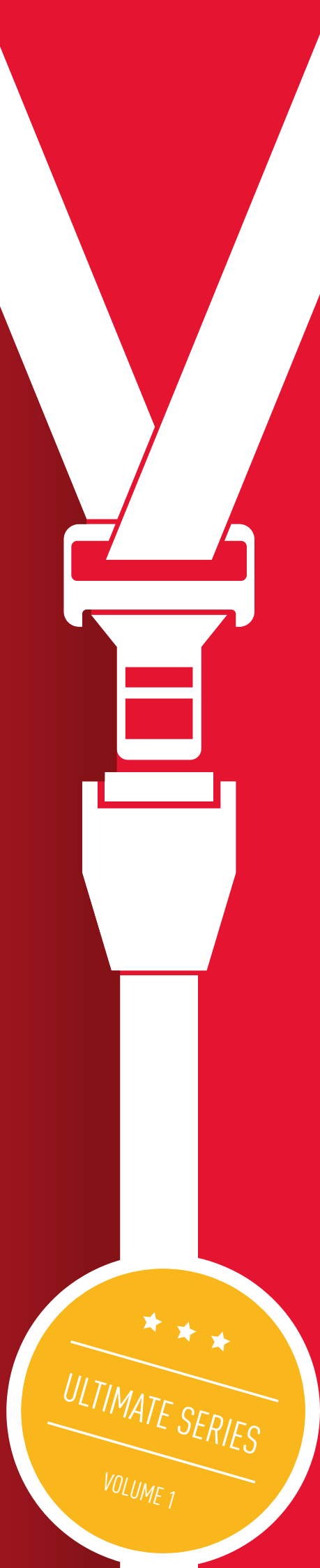
Redspire

The Ultimate Guide to: Security in The Cloud

Post the Apple iCloud hack, is it time to cool down on cloud or not?



The Ultimate Guide to: Security in The Cloud

In the light of the Snowden revelations of the last 18 months, many businesses have started to feel that the onward rush into all things 'cloud' may prove to be somewhat premature.

This uneasiness may have been further compounded in some people's minds by a couple of unexpected crashes of both the web and even Microsoft's core Azure cloud service this past summer. At the same time, there are the seemingly endless high-profile stories of prominent websites and services being attacked, sometimes successfully, by hackers.

There was a genuine sense of shock in many quarters, as well, when celebrities' very personal data was stolen from Apple's iCloud service. Popular web-based email services like Gmail have also been accused of being too porous and open to prying eyes, forcing companies to step in and impose security patches.

Clearly, if you feel that putting your personal data out into cyberspace is riskier than you might like, putting your customer data – let alone your company accounts! – into the cloud may start to seem genuinely dangerous.

It is rational to be very cautious when it comes to computer security. It is even more rational to fear the consequences of being found to be lax when it comes to handling customer data.

The UK's data privacy watchdog, the Information Commissioner's Office (ICO), has been exercising its power to fine companies up to £50,000 for data breaches.

You may be even more concerned to hear that with the EU's proposed harmonisation of data privacy rules across all of the Union, the so-called General Data Protection Regulation - or GDPR - those penalties could rise to 5% of your turnover.

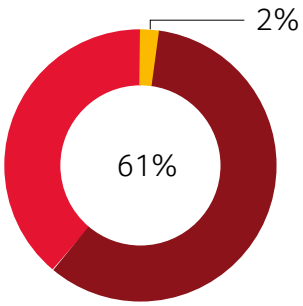
The question is clearly coming into focus, then: is it best to avoid the cloud if I have a mid sized or growing business – is it simply too risky?

Lots of worry. How many actual instances, though?

The question deserves to be evaluated with as much objective evidence as possible. If the cloud, with all its advantages, is rejected out of hand by your company, do you stand to lose more than you would gain by sticking with on-premise alone?

We can attack this question by starting with a look at what the risks really are. How many companies, for all their genuine fear of losing data in the cloud, actually have? The answer is that apart from examples like the iCloud celebrity issue, not that many have.

For example, Cloud Industry Forum research suggests that a lot of cloud fears may not be based in reality.



For 61% of the 250 senior IT professionals contacted, data security was absolutely confirmed as their major worry about the cloud. Yet the same survey also confirmed that only 2% had actually experienced any form of cloud service-related security breach.

As the Forum commented at the time:

"Although more businesses than ever are open to cloud to some extent, turning the perception that cloud is insecure will take time."

Of course, it could well be that the reason why there hasn't been that much data lost out of cloud storage is because there hasn't been that much actually put there yet.

But, again, objective research does suggest the cloud continues to be seen as the default option for more and more organisations. The UK public sector is now recommended to try a 'cloud first' approach', for instance, where the onus on the Whitehall mandarin is to try and source new ICT products off the government's 'CloudStore' buying framework. Wherever possible, organisations ought to choose a cloud-delivered service when they do buy.

Government getting keener and keener on cloud

Actually, the fact that UKHMG is so keen on the cloud should be somewhat reassuring. For many years, civil servants have baulked at working with any kind of system that they did not think had impeccable security. This reserve, which came to be mocked in some quarters as equaling a need for everything to be 'gold plated', acted as a major block to any access to government contracts by third parties (especially smaller IT vendors).

And interestingly, Microsoft - not only a huge player in IT in general but increasingly a force to contend with the cloud - has kept up with this form of accreditation. 18 months ago, for instance, it was able to confirm that its Office 365 cloud service had been awarded the important IL2 security badge. Microsoft is also (as of April 2014) the only CRM vendor that meets the strict EU privacy criteria.

For some IT managers, that will seem like a contradiction in terms, given some of the widely-accepted 'back doors' that programmes like Internet Explorer (IE) suffered from for so long. But that is a reflection of the past, not today. Today, indeed, Microsoft takes security very, very seriously – especially web and cloud security. (And now you can access Microsoft CRM from other browsers, not just IE - which should ease the concerns of those who don't trust it.)

Another issue that often comes up in cloud debate is lack of clarity over where your data is stored. Again, Microsoft has never been anything but very clear and consistent here. The primary data centres for all Office 365 and Microsoft Dynamics CRM Online services are located in its Netherlands and Dublin data centres. For its Dynamics system - the one you would use if you elect to work with the company's Customer Relationship Management technology - the vendor provides what it says are not just market levels of security and privacy, but industry leading ones for both personal and commercial usage of its wares.

The company has also specifically stated on a number of occasions how seriously it takes its mission to safeguard your data too. Thus you may be interested in the statement it issued in June 2013 to queries about its stance towards government surveillance of customer mail:

"We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition, we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security programme to gather customer data, we don't participate in it."

That last sentence is significant: Microsoft is saying – even if you don't believe it – that it does not willingly collaborate with agencies like the NSA. The fact that such agencies, with technologies like its PRISM project, may have been able to siphon off data without its knowing is a separate issue.

And it's an issue Microsoft immediately moved to address.

In November 2013 it strengthened the encryption protection for all of our services and by end of this year, 2014, it will double the encryption key length for all its services, making it much harder to penetrate its systems.

It also announced – in a move that surprised many industry sceptics – that it pledged to enterprise customers that if any government came to us in a national security investigation it would turn the government down.

The company's chief lawyer, Brad Smith, EVP and General Counsel, has also gone on the record to strongly defend this position.

"Our policy is very simple and it's clear: we have no back doors to our software, we do not provide governments with encryption keys to our software [and] we do not help governments break encryption for our software. We have never, not even once as a company, been obliged to turn over to the United States government in any kind of national security matter the content of such an enterprise customer without first notifying the customer and getting the customer's consent. We have never been obligated to do that. And we'll continue to take the position that we should not have to do so in the future."

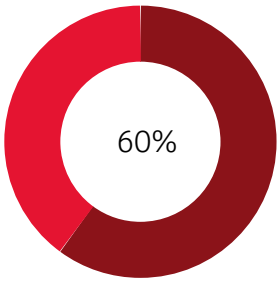
The reality is that Microsoft is a firm believer in security and privacy – and that goes doubly so for the cloud. Microsoft's majorly upped its security 'game' in a way that should genuinely reassure both commercial and personal users of its products and services.

Fear, uncertainty, doubt – are they really helping you?

Let's come down a level or two and look once again at what cloud, security and CRM should mean for the business person. The bottom line question has to be, is there a risk in moving to a cloud-hosted CRM system and placing at least some data in the cloud - or not?

The honest answer is that no computer vendor can genuinely say this is 100% risk-free. Of course they can't. But let's go to the other end of the spectrum. How secure is your data now – in the office?

The very fact that you have a cable and a wireless network connecting you to the outside world technically makes you vulnerable to some sort of cyber attack.



Government data confirms 60% of small businesses were at least cyber-stalked in 2013 alone, cloud or no cloud.

If you have an IP-based phone system, you may also have a potential open door there for the determined criminal.

But – and it's an important 'but' – just as you can take protection for your on-premise systems, you can take out safeguards for your cloud activity. Actually, the beauty of the cloud is that it isn't actually 'you,' but Microsoft, with its deep resources - which it is applying to making the data centres it holds your information in as safe as they are efficient and powerful.

There is also the indisputable fact that the cloud is, in essence, your very own business continuity system. If you spill hot coffee all over the server under your desk and that box contains all your system data, well, that could be very unfortunate if you don't have a back up! With a cloud option, replenishing your data is as simple as a few clicks. By the same token, if your best salesperson leaves the laptop with the fantastic, contract-clinching PPT on it and that was the only copy, that sale is also likely to be in a lot of trouble. If it was all backed up in the cloud, getting that back in their hands ready to wow the customer is as simple as them zipping into the nearest PC World and restocking with some new hardware, then downloading what they need.

There are many advantages to working with the cloud including cost, administration, convenience, as many observers keep telling us, from central government to the private sector. That doesn't mean it is always the right answer for every problem.

Letting security concerns stop you from making any positive move forward into using the cloud would be overly cautious and could actually harm your company in terms of missed opportunity cost.

Pragmatic steps forward

We have tried to objectively assess the concerns high profile incidents like the Apple iCloud breach have raised in many people's minds around the lack of readiness of cloud for real usage, especially by businesses.

We have acknowledged that it is rational to have such concerns, but the objective evidence out there is that despite one or two real incidents, so far cloud has proven to be a lot more reliable and indeed safe than many observers expected.

We have also looked at how a major vendor like Microsoft has responded in a highly proactive fashion to these concerns, the steps it has taken as a corporation to work to address them, its stance as regards data privacy and its parallel investment in the latest technology to buttress its defences.

Our contention is that cloud, especially for a responsive, real-time, flexible system like CRM - where the value-add is its ability to connect remote or field staff securely and quickly with your overall systems - is a potentially highly useful technology that really is worth looking at.

Our advice is that if you do have security concerns, talk to experts who have built working CRM systems for customers like you, especially around the safe integration of such CRM apps with your other systems.

The verdict's clear: cloud is here - shouldn't be ignored - and with a bit of care and attention, can be securely integrated into your system and solution architecture to deliver the kind of cost and efficiency improvements you need to stay competitive.

Still battling user adoption fears? Download your free guide: The Ultimate Guide to: Why 63% of CRM Projects Fail

Download Now