



Cloud security: is it really an issue for SMBs?



Walter Scott, GFI Software

The advantages of cloud computing are well-documented yet security concerns about this delivery model appear to be dampening its widespread adoption in a number of emerging markets. This is particularly the case among larger enterprises and, one would expect, Small and Medium-size Businesses (SMBs). After all, if the large enterprises – which are in a better position to understand the technology and its application – are concerned about security in the cloud, then surely the smaller organisation must be equally concerned? Apparently not.

Misplaced beliefs

A recent survey carried out among 250 SMBs in the UK provided surprising results.¹ Apart from revealing a disturbing lack of understanding of the terminology of cloud computing, security was seen as the lowest priority in terms of influencing a change in strategy towards the cloud. What needs to be addressed, UK SMBs say, are issues of complexity, pricing and fear of vendor lock-in.

When asking those who do not want to use a hosted or managed service what the main reasons were, 56% said their needs were met by the existing set-up, 44% said the service was too expensive, 30% said the service was too complex for a business like theirs and – confirming the lack of understanding of what

the cloud is all about – 26% said these services were only suitable for large companies. A total of 17% said they couldn't see the benefit of it all while only 12% cited security as a concern.

In another question asking what would encourage them to use a hosted or managed service, only 22% chose a guaranteed high level of security. Better vendor terms (43%), no lock-in terms, no contracts (40%) and pay-as-you-go (31%) were all considered higher priority issues.

The research appears to indicate that the industry's viewpoint on cloud-based services differs somewhat from that of the small and medium business. Whereas vendors have pushed hard on the savings benefits of hosted/managed services, it appears that SMBs are not too convinced. And while the industry percep-

tion is that security is hampering adoption, SMBs have indicated that security may not be so important after all. Why?

"If it comes to the crunch, a business will spend money to grow the business and not to secure its network"

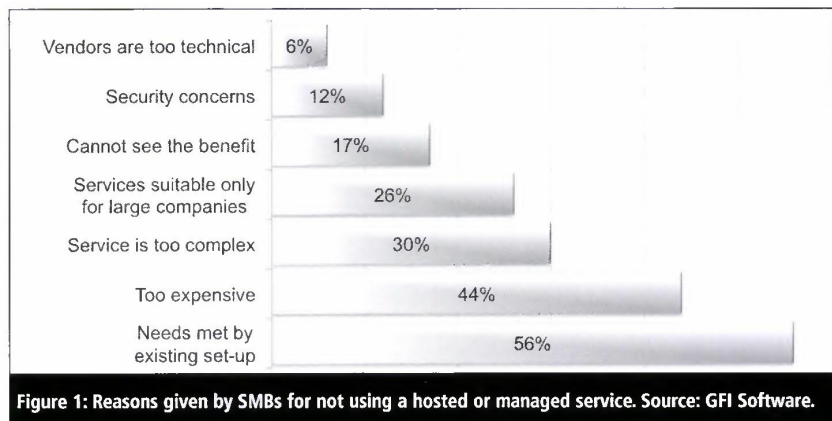
Poor vision

Firstly it has a lot to do with our perception of the SMB. The typical SMB is running on a tight budget, with few resources (financial and technical) and its main concern is the efficient and profitable running of the company. So the primary concern of SMBs is a positive cashflow at the end of the year. This would explain why these companies look at prices, contracts and vendor terms with such scrutiny. Security, in a large number of SMBs, is regrettably often too far down the list to be of concern. If it comes to the crunch, a business will spend money to grow the business and not to secure its network.

But what about those businesses that do invest in security and see this investment as an insurance policy against future losses or security breaches? If they are aware of the importance of the security, the existing threats and consequences, then the security of cloud-based services is surely a pain point (given their efforts to protect their network and data on premise)? Yes and no.

Q&A

Three of the most common questions that the SMB often asks are:





- 'How is my data protected?'
- 'Where is my data?'
- 'Who has access to my data?'

Are these security concerns any different from those that businesses have been facing for the past 30 years? Has anything changed just because the delivery model is now in the cloud?

Logic would dictate not. So while these concerns are justified, they appear to be unsubstantiated because the approach to security should be no different if it's in the cloud or on-premise.

'How is my data protected?'

It is in the interest of every vendor offering cloud-based services that clients' data is secure and protected. In a country like the US, where a lawsuit could result in material punitive damages for a business, cloud-based solution vendors do their utmost to protect the data they are managing. They have to out-perform because they know that a single breach could lead to litigation and significant risk and materially impact the corporate brand.

"If a business's security concerns are being addressed, the location of its data should be of little concern"

Therefore, cloud-based solution vendors not only have the latest technology, the latest firewalls, the best datacentres and the highest levels of redundancy possible, they also apply multiple layers of defence in-depth that your average business can never have. Thus, if the cloud-based vendor can offer such a high level of security that is beyond what an SMB can provide, isn't this concern irrational?

'Where is my data?'

If cloud-based solution vendors are going to extremes to protect their clients' data, rest assured that they are also using optimised mechanisms to replicate and secure that data across multiple disks, servers and locations. If a business' security concerns are being addressed, the location of its data should be of little concern. That

is why this fear is also not justifiable provided the provider is of substantial size.

'Who has access to my data?'

Clients' concerns should focus on how flexible the service provider is in meeting their requirements. In choosing a vendor, the existing security policies adopted must meet the needs of the business paying for the service. Moreover, if the client's security requirements change, these changes must also be reflected in the security policies implemented by the cloud-based solution vendors.

"They see cloud-based solution vendors as the answer to offloading their security concerns. With security no longer a priority, it makes sense that SMBs are focusing on the business aspects of the model"

What has changed with the cloud is the extent to which security policies can change. For example, when employees are made redundant, you would delete their accounts and block all access to the network. When using a cloud-based service, you now also have to block any access rights to the data that is stored in the cloud. The concern that employees could take confidential data with them is the same in both cases. The process to stop that requires additional policies. This is why it is so important that a vendor's security policies are flexible and can change as their clients' needs change.

Is it all the same?

Security issues may have changed slightly with this delivery model but the approach to security should be the same irrespective of where the data is kept – on-premise or hosted/managed in the cloud. The same best practices apply and good business judgement is still required. However, security in the cloud will be better than anything a small or mid-size business can implement.

And this may explain why SMBs are not overly concerned about security

because they see in cloud-based services a level of security that they can never aspire to achieve. On the contrary, they see cloud-based solution vendors as the answer to offloading their security concerns. With security no longer a priority with this delivery model, it makes sense that SMBs are focusing on the business aspects of the model. How much is it going to cost them? Will they be locked-in? How much will it cost to migrate their data if they choose to return to an on-premise model? These are the real business concerns that have a direct impact on the bottom line.

It is perhaps the right time for vendors to re-assess how they position cloud-based services to SMBs and change their messaging.

Food for thought, no doubt, and it certainly calls for additional research into what SMBs really think about a delivery model in the cloud. A readjustment in messaging and a new educational campaign – especially through the media – may contribute to a much wider and faster adoption of this new approach to managing security and boosting business.

About the Author

Walter Scott is the CEO of GFI Software. He previously served as the CEO of Acronis, a provider of scalable storage management and disaster recovery software. Prior to joining Acronis, he was CEO of Imceda Software where he executed marketing strategies that resulted in a successful sale of the company to Quest Software. Scott was also instrumental in Embacadero's successful IPO in 2000. He started his career in sales with Banyan Systems where he contributed to the growth and success that led to Banyan's IPO. Scott holds a bachelor's degree in marketing and a masters degree in business administration from the University of Maine.

References

1. 'GFI Software SME Technology Report 2010'. GFI Software. <http://www.gfi.com/documents/SME_Technology_Report_web.pdf>