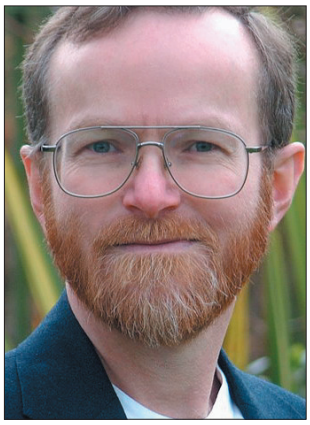
LOCKING UP THE CLOUD

Can cloud-based information ever be as safe as in a data centre? Graham Oakes reports.



Graham Oakes: the people factor

Security has always been tough. Although there are many services that support it (authentication, authorisation, identity management, etc), implementing those services doesn't in itself create security.

Security is a property of the entire system: it relies on those services interacting correctly and every other service using them appropriately. And even then, people will find ways to do stupid things.

This is further complicated by the fact that security is asymmetric. As an architect, I need to secure the entire system. An attacker only needs to find a single chink – a much easier task.

This comes to the fore as services are moved into the cloud. There may be many attractions to the cloud, but security isn't one of them. Data in the cloud just feels less safe than data in a private data centre, behind multiple layers of access control.

So how can a security architecture be built to protect data in the cloud? That may be the wrong question. Absolute protection isn't possible, no matter where the data is stored.

The real question is, can data in the cloud be made as safe as data in the data centre? So let's look at some of the risks that the data is currently exposed to:

- Although the master version is in the data centre, people across the organisation have downloaded copies of it. They extract it into spreadsheets for further analysis. They email it to themselves so they can access it while on the road. These copies are now on laptops, smartphones, USB sticks…The master is secure, but the data isn't.

- Many of those copies are illicit – they're not sanctioned by the security policy. But people need them to do their jobs. Their work has evolved in directions the policy never envisaged, so they fly under the radar. This puts the data doubly at risk: it lies completely outside the corporate security infrastructure.

- Unless within a large organisation, the security team in the data centre is probably small. For a typical mid-sized organisation, it might be one external consultant doing an occasional review. It might be even less. This team can't realistically hope to keep ahead of a determined attacker.

Notice the people factor. If data is moved to the cloud in the right way, it can reduce the need for people to take local copies, and thereby increase its overall security.

Likewise, a shared cloud may have the scale to justify a dedicated security team. For all its risks, the cloud might indeed be as safe as the data centre. Security is about the entire system. That includes the people and processes, not just the services.

● *SOA, Web Services & Enterprise Integration Evaluation Centre Expert Dr Graham Oakes is the principal of content management, product development and customer service strategies consultancy Graham Oakes Ltd. Email: graham@grahamoakes.co.uk. Website:* ***www.grahamoakes.co.uk****.*