Beware of the cloud

RESEARCH

The Cloud is coming to a company near you. Mark Piesing meets Mark Skilton to find out what that means for our security

The Cloud is changing the way our lives work, but few of us have thought through its implications, according to Mark Skilton, former Global Director at Capgemini with more than 30 years' experience in the IT industry, now Professor of Practice at WBS. "Its most worrying aspect," he warns, "is the NSA (US National Security Agency)."

Remote hosting

The Cloud is an umbrella term referring to a product or service that is hosted remotely from the customer and without the need to have expensive hardware and software. The growth of the Cloud has depended on the spread of internet connectivity, coupled with the ability to store vast amounts of data cheaply and then share it quickly on a global scale.

"The world passed one zettabyte of global online storage in 2010," says Skilton. The figures may be huge but the data stored is personal. Data can't care who owns it or what is done with it – but you should do. "Cloud computing has consequences," says Skilton. Data stored in the Cloud can be recorded, even rewritten, and shared around the world phenomenally quickly.

Skilton believes we should be asking "what don't we know about our data that we should?" Do we actually know where our data is being stored? Do we know how to retrieve it if it goes missing? The answers to these questions, Skilton believes, are going to change the way businesses behave and are governed. "It will change employment law," says Skilton. "Rather than being a policeman, the law will have to be an enabler of innovation."

Data protection

Andrew Joint, Commercial Technology Partner at technology law firm Kemp Little, argues employers need "stronger guidance on data protection issues". He believes companies should be asking exactly the kind of questions that Skilton highlights, since the concept of the "layering of provider" means that even if your contract for cloud data storage is with one supplier it is probably in fact running on, say, Amazon with apps provided by a third party.

Joint also says the standard contract "is rather one-sided" in the supplier's favour, and can be summed up as "we are not responsible". Joint believes employers have to be wary of promises to employees about where data will be held and who has access to it.

It is just not sensible, Joint says, to throw data into the Cloud without due diligence, which includes checking "what grade the data is" and whether it is more suitable for a public cloud, where data is shared over a network open to the public, a private cloud that is just for members of an organisation, or a hybrid cloud, where private and public clouds are bundled together but remain separate entities.

Google network room/© Google

Implications for employers

However, what is really driving employers to think about these issues is the attitudes of their employees. According to Kathryn Dooks, Employment Partner at Kemp Little, while more and more employers are comfortable with storing personnel data in the Cloud, they didn't expect employees to raise it as an issue.

"People are much more aware than they thought," says Dooks. "If you are transferring data then you need everyone's express consent if it has not been covered in the employment contract."

For employees any accidental data loss may come down to embarrassment or stress rather than financial loss and, so far, Dooks believes, cloud hackings have been confined to online gaming rather than employee data – "at least in public".

For Joint, the law is going to catch up and "the future is more regulation". Since the NSA leaks from whistleblower Edward Snowden industry – certainly in Europe – has been losing the fight for self-regulation, and a new European data protection directive is on its way.

In the end, Skilton believes, nothing can stop the growth of the Cloud as the economics are irresistible. All we can do is be more concerned with "the ethics of the Cloud" and how it is used. ■