LPM

LEGAL PRACTICE MANAGEMENT

5TH BIRTHDAY EDITION

THE ONLY MAGAZINE FOR LAW FIRM MANAGERS

INNOVATION NATION

AZURE FUTURE

Managing director Andy Michael and head of cloud
solutions Paul Tozer at Quiss discuss being in control and
secure with Microsoft Azure

t doesn't matter how large or small a law firm is, cloud adoption comes down to clients and governance. Protecting client data will always come first.

"When Microsoft implemented the UK regional datacentre, that was really a tipping point, from our perspective. Law firms could now actually start to adopt the cloud model with a bit more assurance about the quality and security of their data," says Andy Michael, managing director at Quiss.

"Lawyers are lawyers," he says. "I don't expect them to know IT or different cloud models; that's where Quiss comes in."

VIRTUAL RECOVERY

SME law firms still hesitate on cloud adoption, whether it comes from the need to sweat an IT asset before moving on from on-premise operations, or being uninformed as to the models and pricing options available.

Quiss's head of cloud services Paul Tozer says firms can use the cloud on a true consumption model, where they only pay for what's used rather than what's provisioned.

"This speaks volumes for law firms because they want to know what their monthly fees will be and have that flexibility to adapt to changes to their practice – if they merge with another company, for example."

But, Tozer says, the biggest misconceptions about cloud that firms have is around control and security.

"When working in Microsoft Azure, users have complete change control and data management – it's all built into the system. For compliance, this is a big hitter."

Azure can handle data access requests directly in its system – it will search not just within emails but also documents and other qualifications. If a firm is doing that on-premise it can be a very difficult process, he says.

Michael says: "Using Azure means that you're replicating your machines, virtually, into Microsoft's cloud, all for the purpose of backup site recovery."

And when backup is synchronised directly to a firm's systems, he says, the recovery point objective could be as low as 15 minutes – that's very disruptive to what was the old disaster recovery technology. Traditionally, someone would have to come into your space, load data into new servers and start them all up – that was looking at a 24-to-48 hour recovery time.

"If you lose your infrastructure, machines can start up insite recovery with the structure actually working out of the cloud – this is one way to prepare for a potentially big cloud migration."

But that's for dipping toes, says Tozer. As part of Quiss's offering, it can do a big bang approach to cloud migration.

He says: "We'll refresh all of your servers, infrastructure and desktops. Where traditional hosting providers use Citrix as their delivery method, we use a modern desktop approach.

"The cloud becomes an extension of your network – all of your application forms live on your local machines but you have what's called an 'express route' to the cloud servers. It just becomes another office."

And if you want to enable people to work remotely, Tozer adds, you can lift the machine off the network (hosted in the cloud), which has an always-on VPN and that user can work anywhere as they would work in the office.
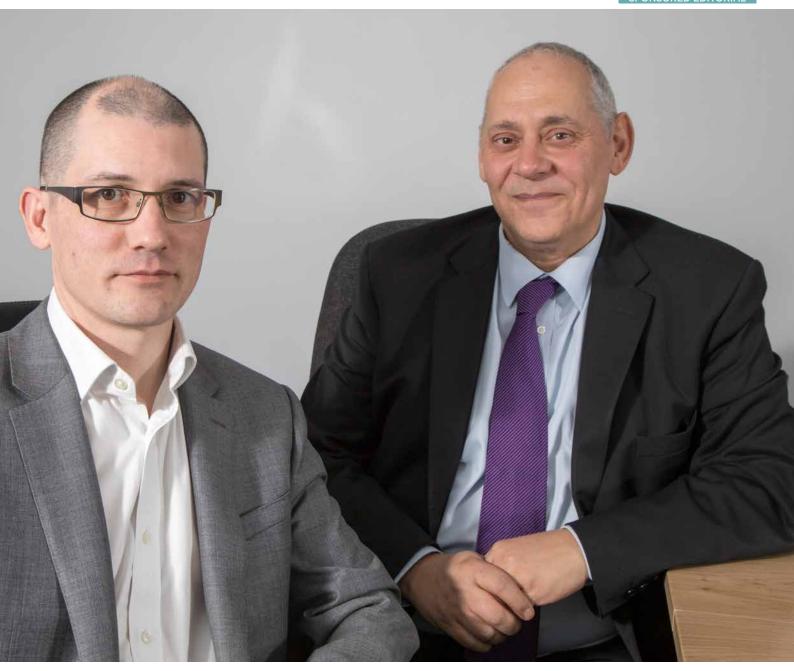
SECURE IT

Security in the cloud remains a top area of concern for legal leaders. Michael says, looking at cloud security from a business perspective, no matter how a firm works, they're all connected to the internet in the same way – so who is better placed to secure that environment, your internal people or Microsoft?

"A lot of people think that because they can't touch it, it's out of their control and therefore anyone can hack it," he says.

Tozer agrees: "Microsoft employs a lot of security engineers and their intelligence comes from not only Office 365 but also Xbox live, Hotmail, Bing, MSN and so on. They have multiple systems and people working on threat detection and prevention."

He says the SME market, by contrast, can only afford to hire a handful of people for IT in-house, if any at all. And those teams are more geared toward the day-to-day running of IT and usually aren't equipped to focus on security in the same way.

It's also important to understand that all communications between end-user device and your server are encrypted – it's not easily hacked, says Michael. "It would take NASA or the CIA to sit and run algorithms for weeks to find out that you emailed someone something."

And it's not just encryption, Tozer says. There are added features such as two-factor and multi-factor authentication that can be switched on – really increasing security more than you could

on-premise and a whole lot less painful to implement.

The same goes for managing the machine while it's out of office. "Microsoft Intune can manage a device when it's not on the network, so if you lose a laptop, it can be wiped remotely. Laptops are also encrypted using BitLocker. So there are multiple layers and opportunities for further security," he says.

Michael adds that some people just don't like the idea of the cloud, however they're probably using it already.

"Almost everyone is using cloud computing in one form or another. It's part of our lives now – how we use it is more important than the fact that it exists. And the benefits that it will bring in the future are going to be determined by how we use it."

It's changing fast. Michael says there are many features being introduced in Azure Logic Apps. There is so much of it coming down the line, and it's all designed to make firms' lives easier. **LPM**