



SECURITY

With the number of mobile devices continuing to expand and cheque books and cash becoming less common as money increasingly flows through cyberspace, the issue of trust is becoming vital.

At last week's Infosecurity event there was a lot of talk about the need to secure the cloud and ensure that remote access is delivered via robust gateways, and at the heart of it was the question of identity.

As the perimeters of security have widened over the past few years to surround multiple access points and the individual, the challenge the industry faces is to ensure that only the right people can access the network.

Identity challenge

"A recurring theme has been the concept of trying to establish digital identity, and that will be one of the greatest challenges to emerge in the next decade," says Barry Jaber, assistant director of strategy at PricewaterhouseCoopers (PwC), which has been charged by the government-backed Technology Strategy Board to identify future security trends.

As well as identity, PwC expects to see several other developments over the next decade (*see box, p10*), but identity is the one that stands out among the list of predictions.

"New technology has made it easier to impersonate people, companies and brands, and that is a real threat," says Jaber, adding that trust is crucial – and not just between people. As the volume of data continues to grow, there will have to be trust between different technologies. "There have to be different ways of establishing trust," says Jaber.



FREDERIC SIERAKOWSKI/FLEX FEATURES

Securing our digital future

Identity protection will play a key part as IT advances our digital world, writes **Simon Quicke**

"Current models primarily look at human-to-human trust. But with greater connectivity, there is an increasing need for humans to trust technology, technology to trust technology, and even technology to trust humans, as devices increasingly act on behalf of individuals," says Andrew Tyrer, who heads the information security activities at the Technology Strategy Board.

The reason that trust is so vital is because security fears are holding back cloud adoption. And as we move towards more micro-payments via wireless devices, users need to be confident the method is safe. And for

companies, the days of keeping all the staff in the office are over.

The predictions made by the Technology Strategy Board are designed to help British companies work out where they can take the lead by using information security. The report shown at Infosec suggests the largest opportunity is around nailing this identity opportunity.

Digital future

RSA, which is well known for the tokens carried around by many corporate staff on their keyrings, used the show to display authentication systems that do not require hardware.

Cryptocard, another authentication specialist, demonstrated its cloud-based Crypto-Mas offering which users can access using software tokens already downloaded on their smartphones and laptops.

So the industry is moving to do something about the identity issue, and authentication is developing to focus more on making life easier for the individual but equally secure for the provider of data.

But despite such advances, more will have to be done to ensure that the world the Technology Strategy Board is expecting to emerge by 2020 does so. "The cost of inaction will grow



and the [consequences] of under-investment or delayed investment will become more severe over time," warns Neil Hampson, a partner at PwC LLP, who was part of the team commissioned to write the report.

Channel role

For those in the channel operating on the front line, the issue of trust has already cropped up and is causing security resellers to confront technology changes and shifts in society.

Barrie Desmond, business development director at VADition, believes that what was seen as criminal 30 or 40 years ago is no longer perceived to be stealing, particularly when it comes to intellectual property. And the generation of 'digital natives' is struggling to understand that not everyone is trustworthy as they bandy around all sorts of personal information.

But Desmond says that with demand for web 2.0 security only likely to increase as awareness of cloud and social networking grows, resellers can strengthen their offering by adding security tools.

But the key to making protection widespread is to get away from the complexity and hurdles that security solutions often present to the user. "You have to make it easy to use, affordable and easy to deploy," says Gary Marsden, vice-president managed services at Cryptocard.

The gauntlet has been thrown down to the security industry to be picked up and carried well beyond Infosec. The importance of cracking the digital identity nut goes well beyond the security industry, and those in retail, government and the finance sector will be watching and hoping a solution emerges before 2020.