INSIGHTS
Tom Crampton, CEO of TrustedImpact

"In 2005, 'Cyber Security' wasn't really a word that was used and neither was 'cloud'. There's a comment you'll often hear information security professionals say which is "there is no cloud, it's just someone else's computer" - which is true.

Not too long ago, we did a study to gain insight from key individuals across the private sector, government and small business to understand how they approach adoption of cloud.

Adoption of cloud computing capabilities including SaaS offers substantial opportunity to every type of organisation, especially smaller organisations, to improve Cyber Security posture in ways that previously weren't possible.

From this study, we found that 100% of those organisations we spoke to were embracing cloud services and 40% of the organisations said that the information they were migrating to the cloud was considered sensitive.

43% of the organisations reported that they did not discuss cloud-based risks at a board level. This revealed that, generally, IT departments were doing a great job at embracing cloud but important business considerations surrounding risks to the reputation of information and interactions, hadn't made it up to the executive level.

This means that, in those circumstances, board and c-level executives weren't discussing the unique risks associated with cloud environments.

The biggest issue we learned from this study was, what we consider, "high trust low proof".

Around 80% and 90% percent of the organisations believed cloud service providers had disaster recovery plans and incident response plans respectively but less than 41% knew whether or not the plans had been tested by their relevant cloud service provider(s).

These revelations are not surprising given we, and our information security peers, so often hear "what - we should test our backup? Why would we do that? It might not work" - and this is the point.

If you don't test these types of plans, there's a good chance they may not work when an organisation needs them most. So you do want to test them, to make sure they will work."

CYBER SECURITY LEADERSHIP PANEL SERIES