



cutting through complexity

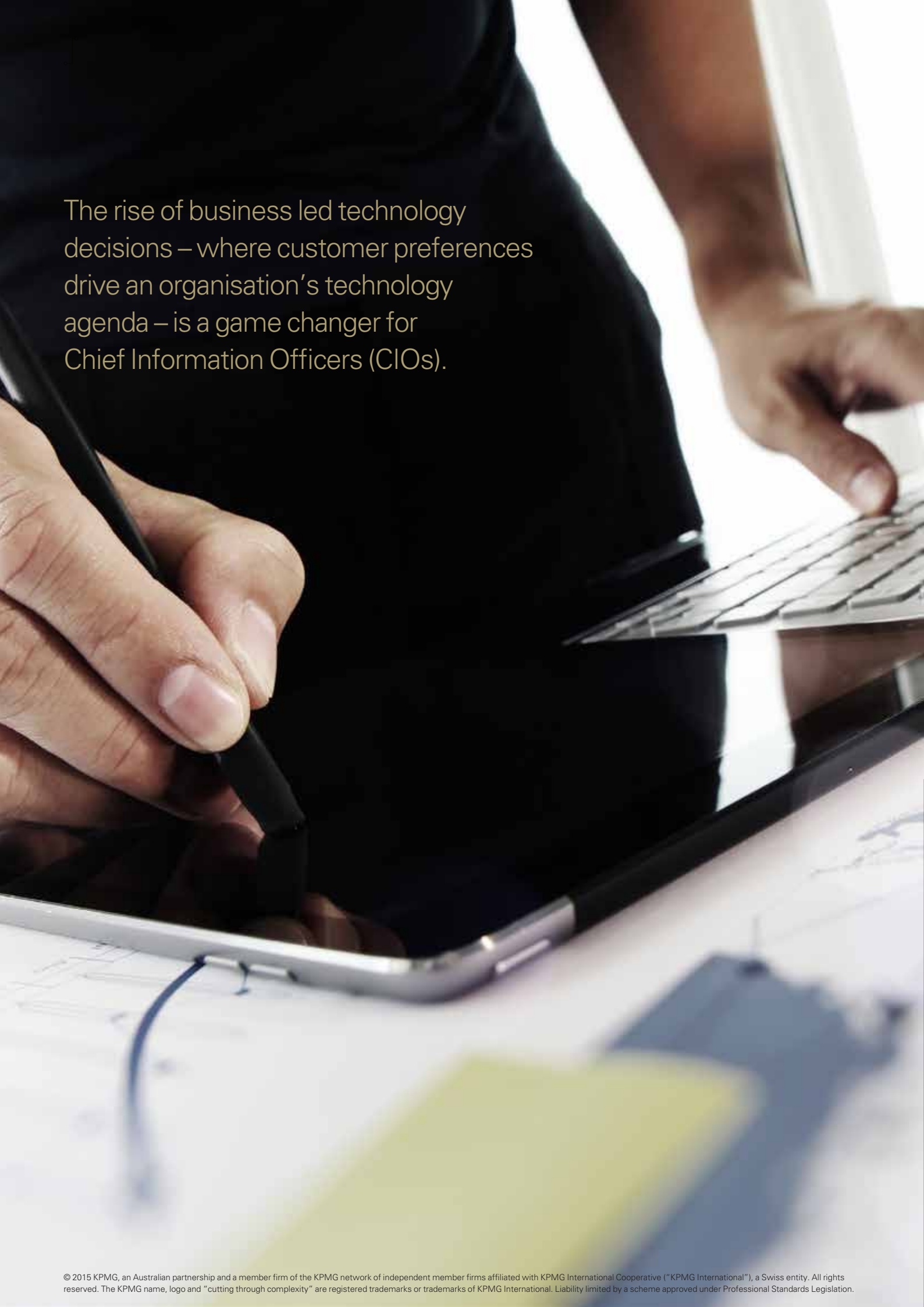
The CIO challenge

Driving business and technology collaboration to deliver growth

June 2015

kpmg.com.au



A close-up photograph showing a person's hand holding a black stylus and writing on a tablet. In the background, another person's hand is visible typing on a laptop keyboard. The scene is brightly lit, suggesting an office or collaborative workspace.

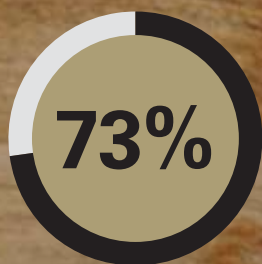
The rise of business led technology decisions – where customer preferences drive an organisation’s technology agenda – is a game changer for Chief Information Officers (CIOs).

The business technology challenge

The most successful CIOs are those that implicitly understand the organisation they serve. They know what it needs, even if this is not necessarily what the business says it needs. Yet for most CIOs, the reality of developing and implementing a business technology strategy, fine-tuned to a customer centric world, is challenging. It necessitates a new degree of business collaboration – even leadership – and requires a shift in the balance of business and technical skills that have traditionally been considered most important for CIOs.

This is the case whether it relates to digital, cloud adoption, cyber security or IT cost management. It is not surprising then that in the absence of in-house skills, CIOs are increasingly seeking out external parties for help in solving many business enablement issues.

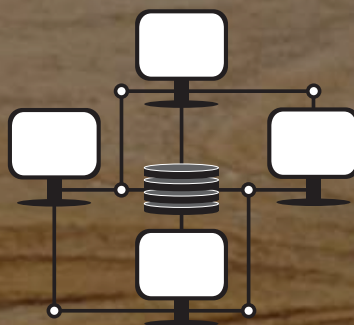
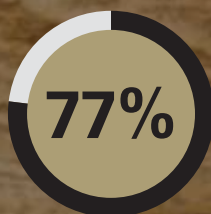
According to a Forrester Consulting study commissioned by KPMG, 73 percent of the Australian organisations surveyed have sought, or are seeking, external support to assist them in resolving the challenges they are facing with their digital strategy: 77 percent with cloud adoption, 79 percent with IT cost management, and 73 percent for their cyber security challenges. We believe this is inevitable in the face of increasing demands on an organisation's technology team.



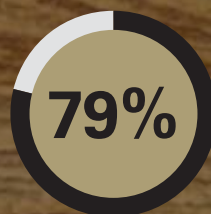
73 percent of the Australian organisations surveyed have sought, or are seeking, external support to assist them in resolving the challenges they are facing with their digital strategy.



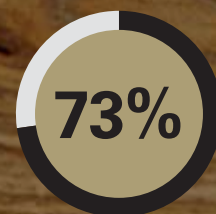
cloud adoption



IT cost



cyber security



We believe this is inevitable in the face of increasing demands on an organisation's technology team.

The rules of investing

The Forrester study showed that almost three quarters of Australian organisations have a digital strategy. Yet only 15 percent of the technology leaders surveyed believed their organisation had the skills and capabilities to properly execute on that strategy.

This issue is compounded by the common perception among business leaders that implementing a digital strategy will be relatively easy; leveraging simple off-the-shelf technology solutions.

A deficit in skills is not the only challenge however. Only 19 percent of CIOs believe they have the right technology to execute on their digital strategy, according to the survey.

Budgetary constraints are always an issue for the CIO and the issue shows no signs of abating, despite the perceived importance of business technology. Yet while this puts an inordinate amount of pressure on CIOs to deliver more with less – sometimes to the detriment of an organisation’s business strategy – we would argue that ‘throwing money at the problem’ is not always the best solution. Certainly there shouldn’t be an assumption that technology will offer a better solution or deliver a productivity benefit.

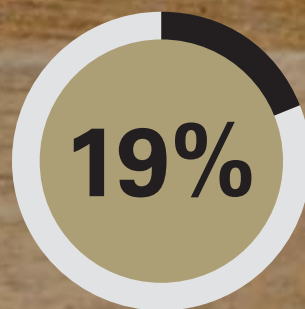
The dot.com boom and bust stands as a cautionary tale of what happens when the normal rules of business are ignored. For all the allure of shiny, new opportunities, it is critical that business understands where the IT dollars are going and what benefit they are receiving from them. To this end, it is imperative that organisations apply a rigorous cost-benefit analysis to each and every investment they make – whether it is a new branch network or physical distribution centre, or online channels.

This is not always straight forward. In the digital space, for instance, business cases are often predicated on the notion that if processes are improved, there will be a concurrent uplift in revenue. Yet these softer benefits are the harder part of the business case to quantify.

Getting it right is well worth it, however, as successful organisations will attest. This has as much to do with the design and implementation of the strategy though, as with the size of the spend. Some of Australia’s largest financial institutions have shown that how an investment is leveraged is more important than the scale of the investment.



Only 15 percent of the technology leaders surveyed believed their organisation had the skills and capabilities to properly execute on that strategy.



Only 19 percent of CIOs believe they have the right technology to execute on their digital strategy, according to the survey.

The need for security

Of course, business technology is about managing the risks as well as the opportunities. Organisations need to understand that while security doesn't deliver an obvious financial benefit, it is a critical part of business enablement; you can't sustain your business or sell to customers unless they are confident that you will protect their data and assets.

Developing a business case to justify the security investment, however, can be a challenge. It is not particularly helpful to assess its worth based on its direct contribution to the organisation's bottom line. Rather, it should include a risk-weighted assessment with a view to the resulting costs if the organisation's security is breached. The question should be: what would be the impact to the business both in direct monetary terms – direct financial losses – and from a reputational perspective? It is all about understanding the downside so the business can factor in an investment to mitigate the risk.

Unfortunately, the growth in threats and increased workload for the security function means organisations can get stuck in reactive mode. They become content with surviving the next threat as opposed to anticipating the threat. Legacy IT is a notable victim of this attitude. Many security architects face a constant battle to fund existing security practices. This is because business tends to view the risks as benign. A common view is that the problem has been solved; there have been no breaches, therefore we are ok.

Yet security, in all areas of an organisation, has to be a constant – a preemptive activity, not a reactive one. CIOs need to explain that while a lot of these systems remain static, the threats are constantly evolving. Thus they require more of a security focus and the necessary investment to protect them.

The challenge for CIOs goes further than this however. Nearly half of those IT leaders surveyed by Forrester said that other priorities in the organisation were taking precedence over security initiatives. Meanwhile, 54 percent said their biggest challenge regarding cyber security was its lack of visibility and influence.

More than money, security is about changing an organisation's culture. The business needs to understand that security initiatives require commitment from a broad group within the business, to change practices right across the firm. Again, it is about preempting security risks, rather than reacting to a security breach once it has already occurred.

Ultimately, CIOs need to deliver a modern IT security practice that is capable of keeping up with the accelerating business driven technology demands. Security should not stand in the way of the business but must be able to support business outcomes while also preserving security.



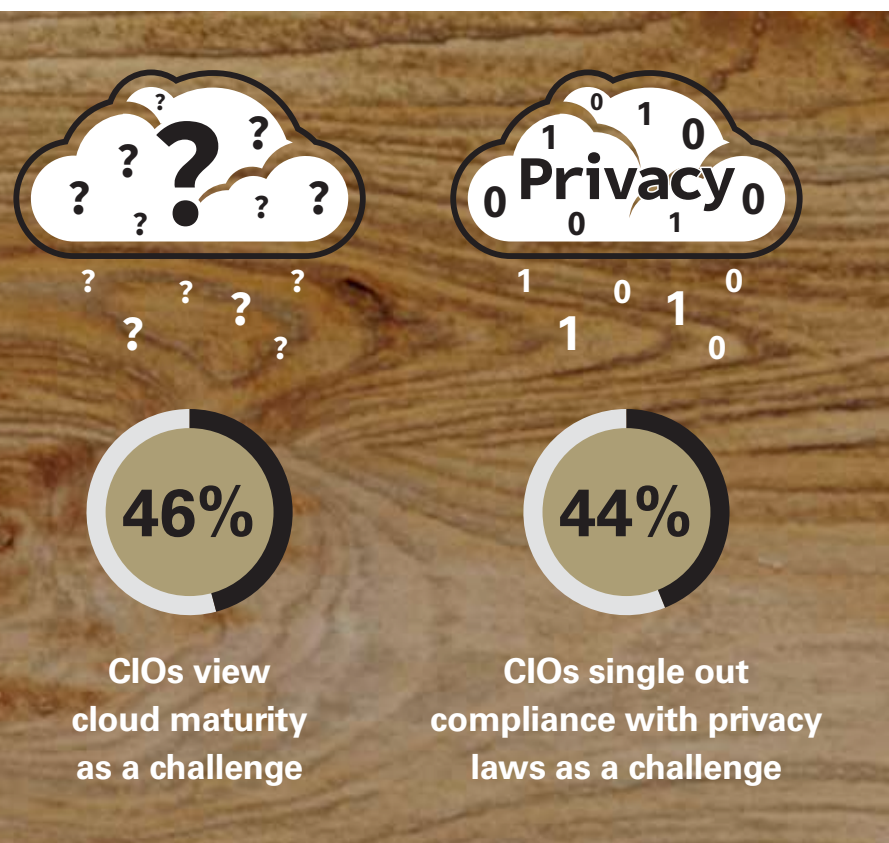
The perceived risks of cloud

According to the study, nearly half of CIOs (46 percent) view the maturity of cloud services as a challenge, while a similar number (44 percent) single out compliance with privacy laws. However, we would warn against such concerns holding sway. The speed of innovation in the cloud services domain is rapid. Organisations should be working on the assumption that any residual challenges will be resolved in short order, otherwise they risk being late to the party and potentially losing competitive advantage.

Organisations need to be proactive. They need to move ahead, understanding how they can leverage cloud services to be an enabler to the business while at the same time dealing with the risks.

Managing the risks is certainly important. Where we see considerable concern is in the way data is stored and who can get access to it. It is a justifiable worry and while it shouldn't stymie the pursuit of business opportunities, it should be an issue for an organisation's board, not just the CIO. Organisations are the custodians of data for their customers, be they a business customer or a retail consumer. They need to give customers a guarantee that all their data is secure, regardless of whether the data sits in a dedicated private environment or in a public cloud environment.

The way organisations choose to approach this issue as it relates to cloud can differ considerably. The business may decide, incorrectly, that it is immune from risk due to its rejection of public cloud; that all data remains within the organisation's own perimeter. Alternatively, the business may accept that people want flexibility and agility in terms of how they access data when they are mobile and give them that capability in a controlled way. The important question for organisations is, which one genuinely reduces the risk profile?



The speed of innovation in the cloud services domain is rapid.

Organisations should be working on the assumption that any residual challenges will be resolved in short order, otherwise they risk being late to the party and potentially losing competitive advantage.

Two-speed IT

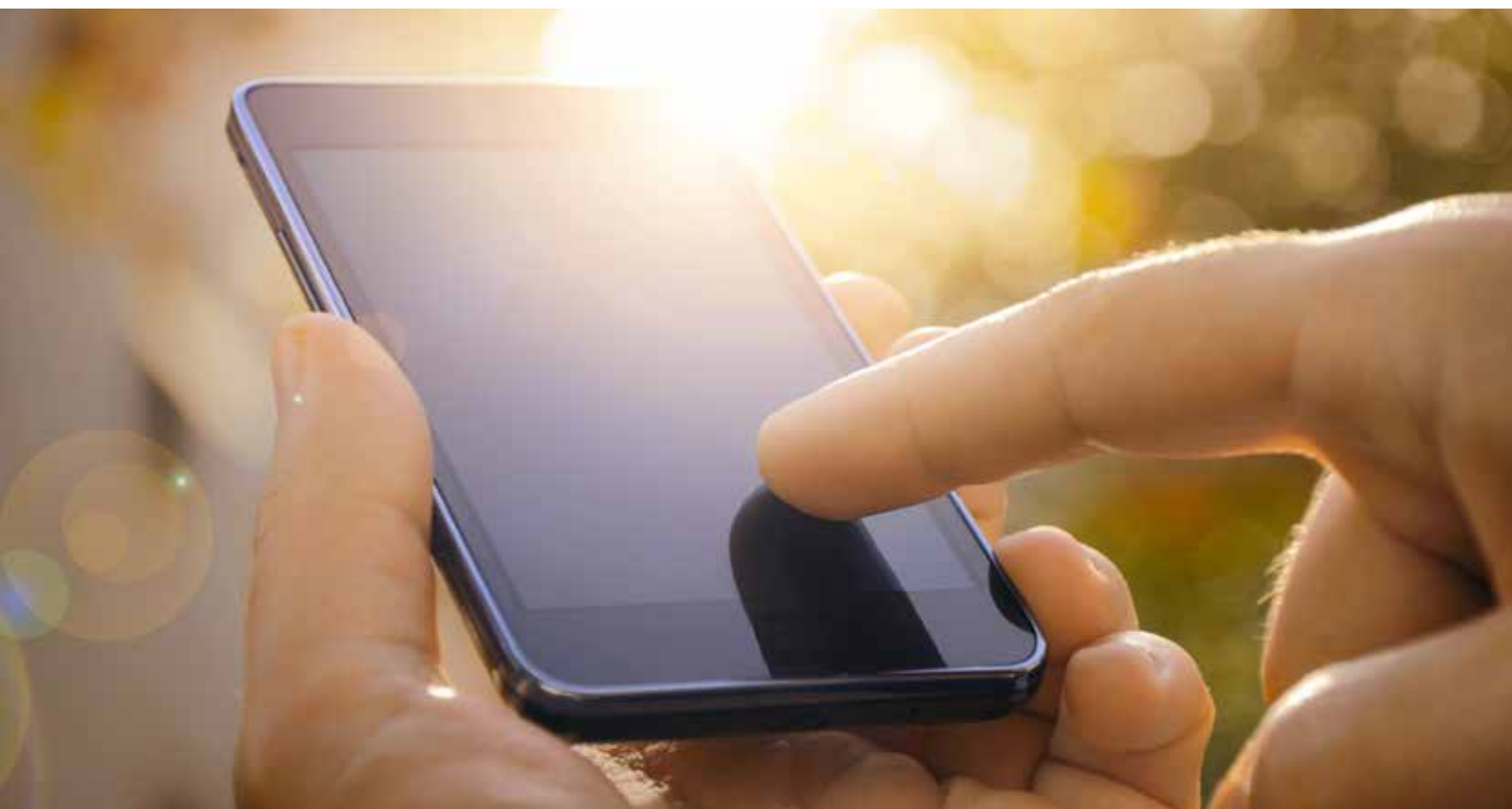
For all the concerns around cloud, the notion of being able to tap into compute and storage capability that is not owned is well established these days and is generally viewed as valuable. This is reflected in the fact that almost half of the Australian executives surveyed by Forrester identified further enhancement of cloud services as a key priority over the next 12 months.

Yet this goes to another issue identified in the survey: a notable number of CIOs (38 percent of those surveyed) are confused about vendors' cloud service offerings.

We believe much of the problem here lies with the fact organisations rely on internal IT capabilities to advise them on any potential move to cloud. Unfortunately the attitude – and hence advice – of traditional internal infrastructure providers within the organisation can be tied to the way they have always done things. Their view is that traditional methods are understood and safe and therefore preferable to cloud which is unknown.

This clearly ignores the benefits that cloud can provide. Yet the failure to understand the opportunities is not surprising. It is an area that everyone is learning about, including the 'experts' in IT. Once again, it underlines the need for external capabilities to assist CIOs in dealing with these issues more adeptly.

It also underlines the two-speed nature of IT today. As CIOs begin to take IT leadership and strategy from the business, we believe it is essential they bring the legacy IT team along with them. Ultimately, the challenge is to connect the more innovative, higher speed business enabled technology with the operational requirements of legacy IT. Finding a solution, however, will take an entirely new approach.



Contact us

Richard Marrison
Partner in Charge,
Technology
+61 2 9335 8156
rbmarrison@kpmg.com.au

Guy Holland
Partner,
Technology Strategy
and Performance
+61 2 9335 7782
guyholland@kpmg.com.au

Michael Bray
Associate Director,
Technology
+61 2 9335 8039
mbray@kpmg.com.au

Andrew Wiles
Partner,
Technology Business
Management
+61 2 9455 9814
awiles@kpmg.com.au

Jonathan Taylor
Partner,
Technology Enablement
+61 2 9346 5696
jontaylor@kpmg.com.au

Mark Tims
Partner,
Technology Risk & Assurance
+61 2 9335 7619
mtims@kpmg.com.au

kpmg.com.au

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

© 2015 KPMG, an Australian partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and "cutting through complexity" are registered trademarks or trademarks of KPMG International.

Liability limited by a scheme approved under Professional Standards Legislation.

June 2015. NSW N12922ADV.