

Time to get serious about digital trust




Australian businesses want the benefits of the digital age. But they are under-investing and under-prioritising cyber security, privacy and data ethics. It's time to elevate responsibility for digital trust to the C-suite.

If the lifeblood of the digital economy is data, its heart is digital trust – the level of confidence in people, processes and technology to build a secure digital world.

So, how are companies doing when it comes to creating this trust? PwC asked 3,000 businesses worldwide about their readiness to address cyber security, privacy and data ethics.

While some are making progress, many can do better. Here's a snapshot of what Australian organisations had to say.


 New investment is not a priority

 Less than a third (28%) of Australian organisations plan to invest in new security and privacy safeguards.

These results confirm our experience that in Australian companies, digital trust functions are under-resourced and sit too far down the management chain.

Given that digital risks do not stand still, it's critical that companies support and prioritise the ongoing development of new controls and frameworks.

Many of the world's leading organisations know this and are investing significantly in strengthening security controls in their products and taking privacy issues incredibly seriously. They recognise that in a data-driven world, where data and technology are fundamental to growth, digital trust is non-negotiable.

 Are boards being properly informed?

 Only 20% of Australian companies are 'very comfortable' that the board is getting adequate reporting on cyber security and privacy risk management.

Considering the complexity of the issues involved, this is a particularly worrisome finding. Without access to the right metrics and insights, some boards could be 'flying blind' when it comes to digital trust.

So what are the key questions that boards need to ask to satisfy themselves that the organisation isn't exposed to unnecessary risk? It's likely they will want to know the business impact of security and privacy activities. For example:

Do we have the right governance structure to ensure that the organisation is adequately protected against cyber risk?

Do we have the right people with the appropriate experience to maintain and enhance our controls in response to changing market conditions?

Do we have a comprehensive plan in place to respond to breaches should they occur?

But boards also need to know how external factors – threats, third-party risk and regulations – affect the company's overall risk posture and the effectiveness of its risk reduction activities. Start with what can be measured today using quantified risk metrics and create a plan to add more sophisticated metrics over time.



Lacking confidence in controls for 'new tech'

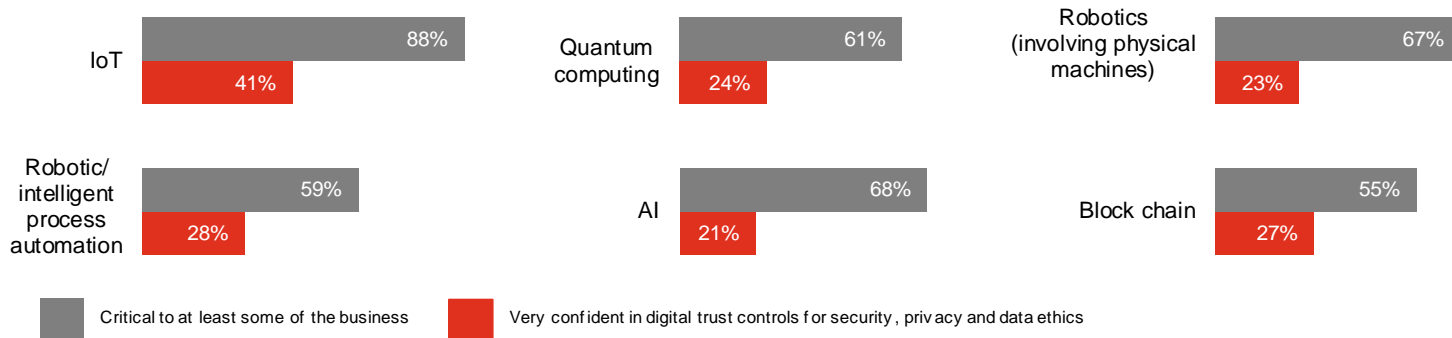
Emerging technology

Most companies are eager to embrace technologies such as the Internet of Things (IoT), quantum computing, robotics and artificial intelligence. But fewer are confident they have sufficient digital trust controls for those tools.

If businesses want to continue to reap the rewards of new digital innovations, they need to do more to manage the downside risk.

68%

say that AI is critical to at least some of the business. But only 21% are very confident in their controls for security, privacy and data ethics around this technology.



Where's the leadership?

A lack of accountability at the top is a core reason that Australian companies are falling behind on digital trust.

24%

Only 24% have a Chief Information Security Officer in charge of enterprise-wide data security. Even fewer (18%) have a Chief Privacy Officer.

Without the right leadership in place, managing risks around security, privacy and data ethics becomes a much steeper climb.

The reality today is that business is data-driven. Management structures need to reflect the fact that digital trust is not a technical issue, but a 'business-critical' issue.

The days of reporting up through the General Counsel, Chief Compliance officer or Chief Information Officer are over. It's time for companies to elevate accountability for the security and privacy of data to the C-suite.



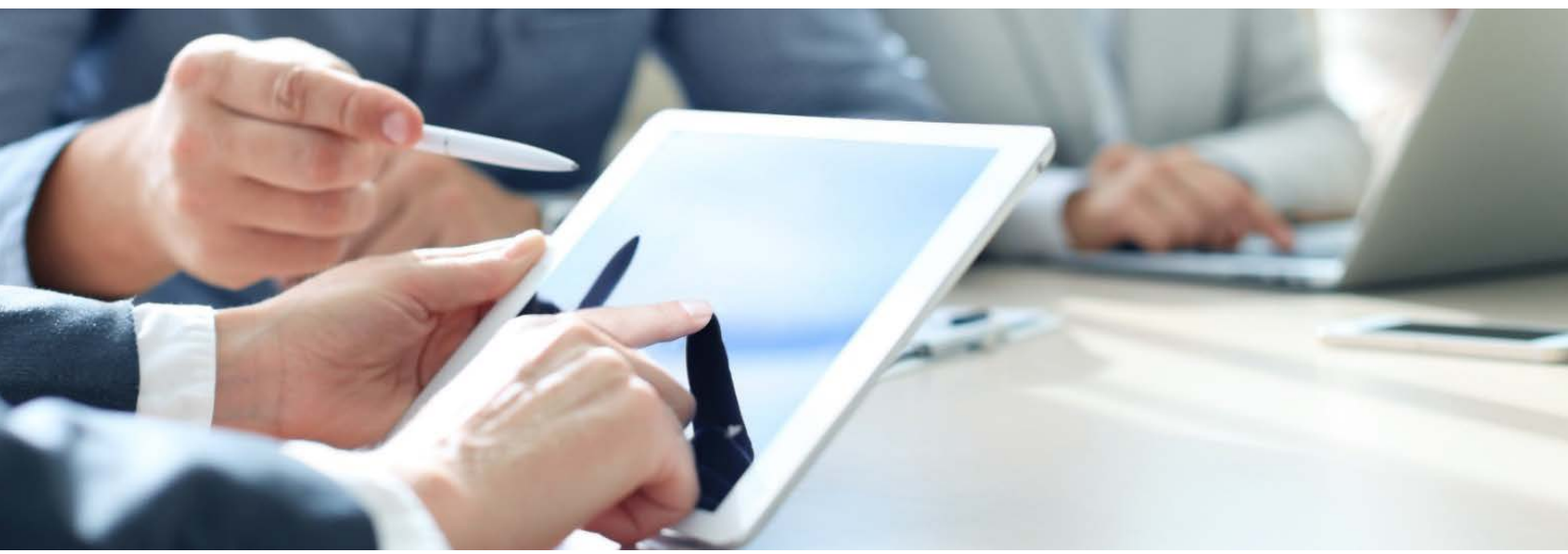
Catch up with the internet

An essay in The Economist predicted 2018 "will be remembered as the year that privacy law finally started catching up to the Internet."¹ But business, it seems, still has some way to go.

Given the growth in new security and privacy regulation and the increasing level of cyber activity, next year will be pivotal as companies globally continue to grapple with the challenge of building and maintaining digital trust.

But those that do – that show the connected world how to lead in safety, security, reliability, privacy, and data ethics – will be the titans of tomorrow. Isn't that a journey worth taking?

¹ The Economist, Towards defining privacy expectations in an age of oversharing, Aug. 16, 2018.





If you'd like to discuss these findings and how they may impact on your organisation please contact:

Peter Malan

Partner
03 8603 0642
peter.malan@pwc.com
Melbourne

Steve Ingram

Partner
03 8603 3676
steve.ingram@pwc.com
Melbourne

Craig Sydney

Partner
02 8266 4938
craig.sydney@pwc.com
Sydney

Richard Bergman

Partner
02 8266 0053
richard.bergman@pwc.com
Sydney

Rob Parker

Partner
02 6271 3484
rob.parker@pwc.com
Canberra

Shad Sears

Partner
02 6271 3438
shad.sears@pwc.com
Canberra

Cameron Jones

Partner
08 9238 3375
cameron.jones@pwc.com
Perth

Jason Knott

Partner
08 9238 3418
jason.knott@pwc.com
Perth

Kim Cheater

Partner
08 8218 7407
kim.cheater@pwc.com
Adelaide

Ryan Ettridge

Partner
07 3257 5373
ryan.ettridge@pwc.com
Brisbane