Q: What is the number one concern you have today when it comes to the state of your organisation's security intelligence?

A: The challenge we have at the moment is too much information. We've got large volumes of information coming from too many different sources. We need to be able to sort through that information. And today we also find it very difficult to determine which nuggets of information are going to be relevant, and allow us then to take actionable steps.

Q: Can you share with us 1-2 examples of how you're ensuring your organisation is more cyber resilient?

A: Across the New South Wales government, transport included, we're required to comply with the digital information security policy. The digital information security policy requires all agencies, and agency heads, to attest to their capability to do five IT security related things. The process will be transparent because the attestations will be in the annual report of each and every government agency. So that's one way in which we're making sure the NSW government agencies and transport and each of transport's agencies has the appropriate IT security capability.

The second example I'll give you is the NSW government data centre. The NSW government has built a redundant, highly secure, highly stable data centre with a back-up facility.

Q: How important is it to work with lines of business on building security into everything you do as an organisation?

A: So I think the debate about how important it is is somewhat passé… we've moved on from that to discuss and debate the hows and the ways in which we can actually engage with lines of business. So part of the digital security policy requires all agencies to have a robust security awareness program, and within transport we're building a three-level program that's focused on executives; it's focused on front-line staff and day-to-day users, and it's focused on our application developers.

Q: Why do CIOs and their IT teams continue to fall short in the way they approach cyber resilience?

A: For us, the challenge really is about translating the myriad of technical gobbledygook that our executives are hearing from many different sources, be they IT vendors, be they consultants, be they our own technicians. Because they're hearing the gobbledygook, and that's usually prepended by the word "cyber", they are paying very little attention to a problem that they don't really understand. The

challenge for us as CISOs is to get much better at doing the translation and making the problem relevant to our business decision makers.

Q: How do you educate the business about data security now that powerful technology is in everyone's hands?

A: So for us it's about both educating the business, but it's very much about educating the users within the business. It's about letting them know about the way in which we want them to use the consumer technology. Part of our challenge is that our users are being told different things by different organisations to which they belong. Many of our users, and particularly our contract work force, may be with transport one day and another organisation the next. I used to call this problem the problem of multiple digital personas, where users get confused about what the expectation is in our circumstance, versus the expectation in a very different circumstance. Our challenge is to make sure that they protect the data our way.