Stuart van Rij

Service provider **security**

JUST HOW SECURE is your service provider? A report this year found that business partners are behind over a third of all data breaches (see the 2008 Data Breach Investigations Report at www.verizonbusiness.com). This was highlighted by a recent embarrassment in the UK when a contractor's memory stick full of user names and passwords was found in a pub car park, potentially exposing the personal details of 12 million users of an online government services portal.

What can you do on the legal front to help protect your sensitive data and stem potential bad press? While only part of the solution, it is critical to get decent security provisions in your contracts with service providers. If you don't, key responsibilities may fall between the cracks and you may be unduly exposed if there is a security breach.

A valuable resource for dealing with this in New Zealand are the mandatory security provisions that must now be included in all ICT contracts entered into by UK Government departments (www.ogc.gov.uk/documents/PPN_Data_Handling_Review.pdf). These mandatory clauses are relatively comprehensive and are intended to reflect best practice. They also provide a helpful benchmark to check whether there's any security gaps in your ICT contracts that need plugging.

In our experience, many of the areas touched on in these mandatory clauses are omitted, or inadequately addressed, in ICT contracts. Here are a few of the key issues covered in the mandatory clause that might be neglected in your agreements.

Are there clear ground rules for dealing with your data?

The key principles and requirements for how the service provider should deal with your data should be spelt out in the contract, or at least in an attachment to the contract (like a Security Policy). The mandatory clauses are relatively comprehensive in this respect. They require conformance to the customer's Security Policy, include specific security requirements, principles and standards in a template schedule, and capture high-level requirements in the main terms.

The mandatory provisions note that care is needed to make sure that any requirement to comply with a Security Policy does not inappropriately constrain the service provider's solution.

Is there a plan for meeting your security requirements?

High level principles and requirements won't necessarily give you the comfort that the service provider is geared up to deliver on the expected level of security. The mandatory clauses go a step further and require the service provider to develop, implement and maintain a plan that sets out the security measures that will be implemented to comply with the customer's security requirements. Of course, it's well known that organisations and their suppliers should have coordinated security plans. In practice, often that doesn't happen.

How will you check that the security measures are actually implemented?

The report on data breaches also found that in 59 per cent of data breaches there were security policies and procedures for the affected system but these were not enacted through actual processes. The moral of the story: Make sure there's follow-through on the good intentions.

The mandatory clauses do this by requiring the service provider to conduct regular tests of the security plan. The customer is also permitted to carry out its own tests (including penetration tests) at any time, without notice. To be reasonable, the clauses provide that the customer's tests must be designed to minimise impact on the services. The service provider also gets let off the hook if they fail to meet the service levels as a result of the customer's tests.

As you would expect, the service provider must change the security plan and its implementation if any deficiencies have been revealed by the tests and the customer has approved the changes.

What happens if there is a security breach?

At the outset, both the customer and service provider should notify the other as soon as they become aware of any breach of security or any potential or attempted breach. Once the service provider is aware of any of these things they should immediately take steps to remedy the situation and prevent it from happening again in the future. The mandatory clauses provide some balance here by requiring that such steps must both be reasonable and include any action reasonably required by the customer.

There are many other aspects of the mandatory clauses that are worth considering. While these types of provisions won't necessarily prevent the loss of a memory stick, they are a critical step in addressing security risks when engaging service providers.■

What can you do on the legal front to help protect your sensitive data and stem potential bad press?

Stuart van Rij is a senior associate at Wigley & Company, a law firm specialising in ICT.
He can be reached at (04) 499 1842 or stuart.vanrij@wigleylaw.com

If there is a question you would like Stuart to answer in relation to IT issues, please forward it to dparedes@cio.co.nz