

## Higher standards may help to improve security of information

### Jim Lee

If a client asks how secure his information is within your firm, do you know the answer? If that answer is based on being “as secure as the next firm”, is this wholly satisfactory?

Clients may be concerned about security and continuity. These concerns are, in the main, not easily translated to criteria for competitive choice. But there is one major influence that changes measurement in the public domain: standards, especially from recognized bodies such as the British Standards Institution (BSI).

While there are few published standards for network and access security that translate into professional practice, there are emerging standards for security in business continuity. Based on the BSI’s published proposals and working papers, the new standards – PAS 56 – will measure compliance for the security and recovery of your business and its documents in the event of disaster. There are communities where compliance will be mandatory.

The Civil Contingencies Act requires local authorities, fire police and ambulance to be compliant. The Financial Services Authority is also taking a specific interest, so legal practitioners should expect compliance to become important.

Let’s look at the differences between document and access security and business continuity. Document security is the more critical concern for clients, yet there are no satisfactory criteria upon which they can rely to compare practitioners. The advent of standards for continuity will mean the client will have a means of measurement.

In the recent past, the Law Society, in conjunction with third-party commercial ventures, committed time and money to a secure network for the exchange of legal documents. The failure of this venture may soon be rued. An electronic exchange of documents without specific action to secure the network against intrusion is frightening. These documents represent the jewels of a client’s intellectual property and commercial contracts.

Technology may be to blame for the difficulties in implementing standards. In secure document exchange here are too many parties for standards to be agreed in the near future.



On the other hand, continuity begins with people. If you deal with human issues – such as where people go – then you can make the technology follow them. Typically at this point the security issues are raised at resolved.

I expect compliance with accredited standards for business continuity will become attractive to the profession even where technology-driven security has been rejected. The evolution of a continuity plan delivers early benefits to the operation of the firm's administration, and these benefits are tangible.

This is not technology for technology's sake but for people – a far more attractive proposition.

Jim Lee is managing director of Campbell Lee plc group.

ENDS

**THE SCOTSMAN**  
**NOVEMBER 2005**