

# Information security

**G**iven the negative publicity surrounding the seemingly endless stream of data breach incidents over the last year or so, it is no surprise that the issue of information security is rising steadily up the public sector agenda.

Organisations realise that they have to do something – and fast – to ensure that highly sensitive corporate information does not fall into the wrong hands. But, to date, all too many have simply thrown technology at the problem, with the deployment of encryption software on laptops being a particular favourite. Unfortunately, however, like everything else in this life, it is just not that simple.

If the underlying causes behind these security breaches are explored, it becomes clear that not one has resulted from an IT failure or even the circumvention of an IT process. Instead, they came about as a result of inadequate business processes and human error, not least due to insufficient staff training.

And this is the nub of the issue. Information security challenges can never be fixed by technology alone because the issue comprises far more than this. What it boils down to is tackling the three Ps – people, places (or physical security) and processes – and each of them has to be dealt with in turn and simultaneously, before automated security controls in the shape of technology can even be considered.

But such activity can be tricky for in-house teams. There is a tendency to lay information security initiatives at the door of IT departments, which do not necessarily have the wide range of skills to undertake them, or of compliance officers, who generally



have little experience of the issues beyond their own remit.

As a result, information security consultants providing specialist bespoke services can play a useful role here. They undertake audits on an organisation's behalf to find out what their particular security risks and threats are. They then devise new policies, processes and procedures in discussion with both the business and IT department to deal with these challenges, before recommending any changes in line with each public authority's own unique requirements.

But it is worth bearing in mind that there are all too many consultants on the market who can end up doing more harm than good. Therefore, checking out any potential partner's credentials, which includes references, is crucial before signing on the dotted line.

Membership of professional bodies such as Institute of Information Security Professionals and The Security Institute, for example, are a given.

Experience in implementing recognised industry standards such as the ISO 27001 information security

## Trusting to the three Ps...

management framework, the BS 25999 best practice guidelines for business continuity and ISO 15489 for records management is also a must.

But it also makes sense to check out any potential partner's attitude to mentoring and knowledge transfer. All too often, organisations pull in third party experts to help them solve their problems but end up with an unsustainable set of systems or processes that they have no idea of how to repeat or maintain. This means that, when the time comes, for example, to update their risk profile by undertaking a new risk assessment, the only course of action left is to bring in a third party again, which can end up being expensive.

Again, what it boils down to is trust. And being able to trust your information security consultants is vital.

Advent IM is an experienced, independent consultancy providing holistic information assurance and physical security services to the public sector.



Mike Gillespie  
Director of Information Assurance

Advent IM Ltd  
Cradley Enterprise Centre  
Maypole Fields  
Halesowen  
West Midlands B63 2QB

Tel: +44 (0)1384 567865  
Fax: +44 (0)1384 566995

bestpractice@advent-im.co.uk  
www.advent-im.co.uk