

Data Dangers

With information security often put on the back burner, Mike Gillespie explains how public sector organisations can ensure that their data is secure.

In light of numerous recent high-profile data loss incidents – most notably the HMRC blunder – a reaction has been sparked throughout the public sector in relation to locking down data. This plans information held within an organisation's network as well as the physical management and storage of data. This issue of information assurance has subsequently been pushed up the agenda, although, in the minds of many senior managers, it is still not a number one priority.

A fundamental issue within public sector organisations is that information security is rarely seen as a necessity in comparison with other corporate initiatives. Established regulations, such as Health and Safety, have been applicable for longer, hence organisations are more aware of the requirements and repercussions should they fail to comply. The repercussions of poor information security are often not fully understood and, as a result, IT is often thrown at the problem in the mistaken belief that it will lock down data and prevent all breaches. This is not the case however, and a holistic, layered approach should be taken to protect data.

The challenge that today's information security officers face is that the rate of which information systems have developed has left data vulnerable to attack from both outside and within the organisations. In particular, the introduction of shared services brings heightened potential for data leakage, so it is all the more important to implement robust security policies and procedures, and to educate staff through regular training sessions, to guarantee the security of information when sharing, accessing or transporting. Security must be regarded as everyone's responsibility, with specific officers accountable for assessment and improvement.

Security policies are core to protecting organisations from attacks – be they malicious or accidental. Policies introduce and specify the do's and don'ts so that employees are clear as to what is acknowledged as best practice when dealing with data, as well as the consequences if policies fail to be adhered to. Public sector organisations should refer to the *Security Policy Framework (SPF)* which contains guidance on all aspects an organisation should consider when protecting information assets. Guidance covers security and risk management and is a recommended source upon which to base local security. Policies generated must be disseminated clearly and regularly so that the entire workforce is meeting the same objectives. While the *SPF* recognises that security policies differ according to the risks faced by each organisation or department, the framework sets out the minimum mandatory requirements; perfect for those keen to implement a new regime into their workforce.

While reports and new initiatives have been issued by the Government since the HMRC debacle, including the *Data Handling Review* and *Hannigan Report*, there is still a general lack of information governance throughout the public sector, even though information management is now fundamental to all activities. That said, the Government is more willing than ever to adopt a holistic approach to security, urging public sector bodies to get the basic right and to build a layered security approach. One Standard which advocates just such an approach is ISO27001. This addresses

information security on a holistic level, from the bottom of an organisation up, and offers an all-encompassing specification which addresses issues of the people, places, processes and technology levels.

A common mistake for those in charge of security is to look to technology for the answer to combat issues as we have said. These people have lost sight of the need for good protective security. Information exists in many formats now, leaving IT as the enabler not the solution to potential risk. One example of best practice is for management to implement a Protective Marking (PM) scheme. By labelling documents with the HMG Markings such as PROTECT or RESTRICTED, one can ensure that information assets are adequately protected, appropriately handled and disposed of securely. Measures such as this do not have to be expensive or technology-based. Instead, by addressing policies, places, procedures and people, those in charge of protective security can trust they are as safeguarded as possible.

In the event of data leakage, regardless of the reasoning given for the loss of information, it is ultimately the organisation whose data has been misplaced that suffers. A holistic approach to data security can minimise the risk of data breaches and the negative affects that come with it. Can you afford to put your service's reputation at stake?

Mike Gillespie is management director at Advent IM