

How Robust Are Your Data Security Measures?

By Robert Mackenzie, Partner, Business Technology and Consulting, Scott-Moncrieff

Posted Wednesday 2nd December, 2009

No one wants to be featured next in the all-too-frequent litany of headlines like -Confidential Data on Stolen Memory Stick or -Lost Laptop Contains Classified Information. Human error does occur, but there are straightforward ways to minimise the likelihood that any such misfortune will cause major problems.

Our on-going experience of working with well prepared organisations, such as the Scottish Government Office of the Chief Researcher, has shown us that robust organisations can put in place some straightforward means of ensuring they minimise the risk of having an IT security breach.

The start point is to ask some essential questions of your organisation.

Key Questions

1. Do you have an up to date security policy which people know they have to comply with and are you confident that everyone knows it exists and has read it?
2. Are your leaders totally committed? Good security has as much to do with cultural issues as technological controls and it is important to have an effective security organisation which is actively promoted and supported from the top of the organisation. This should stipulate clearly defined ownership of systems and data and help to ensure that your own good practice is extended to those third parties you may deal with.
3. Do you have a robust risk assessment process and asset management scheme? Ideally security measures are driven by such a scheme, one that allows you to classify the sensitivity of all the data which you hold. Without this in place how do you know what data to secure, particularly in those situations where it is transmitted outside your organisation?
4. Do you use encryption? In the current climate ideally all mobile devices, be they USB devices or the wide range of laptops available, should be encrypted and someone within your organisation should know where they all are.
5. Do you invest in on-going staff training? For all of these measures to work it is important to educate your staff and ensure there is regular training and awareness rising. This should extend to a clear and easy-to-follow incident reporting procedure which ensures all security incidents are identified and notified to the appropriate part of your organisation.
6. Are you checking the obvious? It probably goes without saying that you should have suitable virus and malware protection in place along with firewalls and, most importantly, they should be extended to the weakest points of any network which are remote users and home workers.
7. Are you keeping it under lock and key? You need to be sure an adequate physical and environmental security over your core IT infrastructure exists, along with physical controls over access to office areas.
8. Who goes there? All of the above needs to be supported with good control of user accounts, limiting 'who can access what' data, including robust password controls or additional, stronger methods of authentication, as required.
9. Are you disposing of data correctly? Having restricted access to your data, it is also important to ensure you dispose of it securely as well. The Data Protection Act stipulates that data should not be held longer than necessary. You need robust measures in place to ensure that data is removed from your systems, and that the devices which held it are also disposed of securely when they come to the end of their useful life.

Case Study

In late 2008 the Scott-Moncrieff Business Technology and Consulting Team was commissioned by the Scottish Government Office of the Chief Researcher. The objective was to provide the Chief Researchers Office with assurance that the data security standards which they, as a government body, are striving to achieve were also being satisfied by their partners in the wider research community.

The report provided a very positive message to the Scottish Government, confirming that, in the main, research contractors had good procedures and processes in place to ensure compliance with data security principles. This appeared to be embedded within the sector, and the existence of the ISO202052 (Market Research Standard) and guidance from the Market Research Society helped reinforce this continual drive towards compliance with best practice.

We identified a number of themes where there is scope for further work and improvement and the two critical areas where there was, not surprisingly, scope for improvement were a wider use of data encryption on mobile devices which could potentially store data of a personal nature, and the need for greater clarity regarding the retention and deletion of research data.

Both of these themes regularly occur in most of the other sectors in which our Business Technology Consultants are involved.

The report itself can be downloaded at www.scotland.gov.uk/socialresearch.

Robert Mackenzie: robert.mackenzie@scott-moncrieff.com or 0131 473 3500