Information Security in the Public Sector

Information Security in the Public Sector is an area that is receiving increasing attention from senior management and Risk Management teams in these public bodies.

In the last number of years, there has been an initiative from central Government to incorporate a Risk Management function in all public sector organisations. This function is to develop a risk register for each organisation, and one of the areas that will feed into this register is that of Information Security.

In order to provide accurate data to the owner of this risk register, the Information Security function in each organisation must have the tools and processes in place to assess these metrics. Reliable and accurate information is a key to the decisions that will be made based on the risk register.

This is not an easy task for many public bodies. In many cases, the area of Information Security is a developing one, and would not have the maturity of the role that would exist in some private sectors such as finance or insurance where there were regulatory requirements that required this role.

The speed with which Internet access to public sector information has been provided is truly breathtaking, even if there are some high profile Internet facilities not yet available to central Government information. This has made it very difficult at times for management to provide adequate Information Security controls to support these Internet based initiatives. Due to the rate at which the Government has adopted Internet based initiatives, it has meant a steep learning curve for the Information Security specialists in the various public bodies.

Standards such as the IS 17799 have assisted ICT Units in many organisations to assess themselves and provide metrics to the management teams. These metrics can assist the management teams in determining how compliant with Best Practise they are, from an Information Security perspective. With this knowledge, they can then assess the project size to gain compliance, or in some cases, certification.

Given the nature of the information that many public sector organisations deal with, knowledge of the details of the various pieces of legislation such as the Data Protection Act 1998 is vital. It is equally important to stay abreast of amendments to these acts. In the case of the Data Protection Act, this has far reaching implications for many public bodies. Not only is compliance with the Act a requirement, it is also imperative that public bodies are seen to be setting example in this area and not to be found lacking.

This can be quite a challenge for many involved in the Risk Management areas in public bodies as the very nature of the bodies can mean they are very distributed throughout the country, and in some cases, internationally.

These challenges must be initially met by having strong foundations from an Information Security perspective. These foundations must be based on an Information Security Policy that has the full backing and commitment of the senior and executive management teams in the body. This commitment must be followed through on with the lines of management that are involved in the day to day operations. Once this policy is in place, and communicated to the staff in the organisation, it will only succeed is there is follow-through with staff awareness. This awareness must be updated on a regular basis to ensure that everyone fully understands the policy of the organisation, how it reflects their culture, and each staff members own role in being compliant with the policy.

Given the number of projects that the ICT units are expected to deliver in a very short period of time, the extensive use of 3rd parties is inevitable. This can mean having people on-site that have their own computers and laptops etc. that need to be connected to the organisations LAN. This can be for troubleshooting purposes, and access to systems via the Internet at their own employer's location. This can introduce a significant risk to any organisation. The primary concern is that of malicious code such as Worms and Viruses being introduced to the LAN. This connection of 3rd party devices effectively bypasses the perimeter controls of the organisation that should prevent hostile or malicious code entering the internal LAN. There are a number of methods that can be used to prevent the unauthorised or accidental connection of these machines to a LAN. These include the use of technologies such as 802.1x, Network Admission Control etc. These risks also highlight the changing threats, and that the classic Armadillo syndrome of a hard outer core and a soft chewy centre is no longer acceptable today. Security controls and countermeasures must be in place at all levels in a network.

The Information Security arena is changing rapidly, particularly for public bodies that are grasping the Internet as a delivery channel. The challenge for the Information Security and Risk Management teams in these bodies is to be aware of the issues and threats, having appropriate countermeasures in place, and keeping up to date with the developments in this area.