Information Security Now - 12

John Mitchell

The key to the problem of data leakage can be laid squarely at the door of poor information security governance. As information security governance is a sub-set of IT governance, then the starting and finishing position rests with the CIO. I am constantly amazed at CIOs who have no clear governance programme in place to ensure that their function can not only support current business objectives, but also help to extend the enterprise into the future. After all, IT departments only do two things: facilitating the development of new business solutions and delivering existing solutions to its clients. In order to do these it must have a suitable organizational structure, excellent staff who are managed by appropriate policies, standards and procedures and a relevant way of measuring performance. So IT governance is all about putting a framework in place which enables the management of IT to meet business objectives with suitable metrics to know whether we are successful. Rather than reinvent the wheel each time it makes sense to pick up best practice from throughout the world and this is where the International Standards Organization (ISO) comes to the fore. As IT only do two things and as the way they deliver these things is pretty much the same regardless of language, culture, or technological maturity it seems an ideal candidate for a number of ISO standards. And this is exactly what has happened over the last decade. There are now national and international standards for IT governance, software development, service delivery, information security and business continuity. Indeed the whole of information technology is now covered by just five standards. The standards themselves have a standard format: Part 1 is the code of practice and Part 2 provides guidance on the implementation of Part 1. All the standards require some sort of policy statement and as a policy is simply a statement of intent these should be concise and to the point. For example, there are only two possible security policies and as they are mutually exclusive your company can only adopt one of them. The first states that everything is open to everyone unless specifically restricted, while the second states that everything is locked down unless specifically derestricted. The implementation of either of these policies will then require the adoption of appropriate standards and procedures requiring the identification of assets which are either to be restricted, or opened up and the allocation of appropriate privileges to the people (or systems) who are to be allowed access.

Apart from the official standards there is a host of good practice out there which has been identified by the Information Systems Audit and Control Association (ISACA – www.isaca.org) and the IT Governance Institute (ITGI – www.itgi.org). These two organizations use a common umbrella open standard titled Control Objectives for IT (CobiT) which sits above the international and national standards and provides examples of good practice and measurement frameworks to enable organizations to implement good IT governance in an economical way. As an assurance professional (auditor) I tend to use a fairly simple process to gauge the governance maturity of any IT function. This is based around the maturity model concept which was initially developed by the Software engineering Institute of Carnegie Mellon university and extended by

ISACA to cover the major IT processes. Basically you can take any process and measure it on a scale of 0 through 5, where these are paraphrased below:

0 = nothing in place to manage the process
1 = initial consideration is being given to process management
2 = the process is repeatable, but depends on individuals for its success
3 = the process is defined and documented
4 = the process is managed and measurable
5 = the IT process is integrated with the business process.

You will immediately notice that full compliance with any of the standards forces the IT function to level 4 as not only is the process defined (which protects against staff changes), but it is also measurable because all the standards require the collection and analysis of metrics to prove compliance. Interestingly, compliance with the Sarbanes Oxley Act requires level 4 conformance. Some of the standards, particularly ISO 27000 (Information Security) and ISO 20000 (Service Delivery) ultimately move the IT function to level 5 by integrating the IT processes with the business processes. ISACA has defined 34 common processes used by IT departments and provides a maturity scale definition for each one. This enables me, in conjunction with IT and the business, to quickly assess the function's maturity in the key areas. It is then up to the business to decide whether they are satisfied with their current level, or would like to improve on it. ISACA also provide an anonymous benchmarking service which enables companies to ascertain how they compare with other companies. I was a bit shocked to find that the average for Information security was 2.8 which is below defined process! Worrying isn't it?

John is Managing Director of LHS Business Control, a corporate governance consultancy which he founded in 1988. He is currently a member of the BCS Specialist Groups Executive Committee and a former chair of the Information Risk Management and Audit (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454