Information Security Now - 6

John Mitchell

Nationwide lose the personal details of 11 million customers on a stolen laptop and refuses to disclose the details of what was stolen. Revenue & customs lose the details of half the UK's population, but at least comes clean as to what has been lost. Over 60 detectives (more than are put onto a murder investigation) are then tasked with searching for the two missing CDs. What shambles? Data is leaking from organisations in a flood and yet the government still wants its identity database; link-up patient records on the NHS; increase voter participation by using systems that are so weak that the Electoral Commission says they should desist; provides for unprecedented access to our DNA and outsources its support desks to foreign companies in foreign lands. The lunatics are running the asylum and us security professionals are wringing our hands in despair at the utter disarray that is presented to us. ISO 27001 recognises that you can control technology, but only manage the people (at least until we get them chipped at birth). However, governments love technology as it provides demonstrable proof of their being in the forefront of developments. It shows that they understand the advantages of IT and can deploy it at a whim. Nice try governments, but you ignore the people side at your peril. HM Revenue & Customs state that its "shared workspace is extremely secure with several layers of both physical and technical security measures in line with the International Security Standard ISO 27001". You notice "in line with", which is not the same as saying "complying with" or better still "accredited to". Nice try HMRC, but we can defrag the English.

I once had a CIO state to me that his department "complied with ISO 27001". A quick gap analysis revealed this not to be the case, but he had been using the "comply" word to his Audit Committee for years and they had interpreted this as being "accredited to". They were pretty annoyed when I explained his sleight of English, but I suspect they were more annoyed with themselves for falling for it. I use the Capability Maturity Models (CMM) from CobiT[1] to explain, in a non-technical way, where the company is on the security continuum. Level 0, no chance. Level 1, scared enough to start doing something. Level 2, something is in place but it is reliant on individuals, Level 3, defined processes which are independent of individuals, Level 4, managed & measurable (now we are talking!), Level 5, IT security is optimised with other security processes within the enterprise.

Level 5 would include security over End User Computing which is where the real risks reside. As stated earlier, it is the people aspects that kill security, not the technological wizardry, so security must be all encompassing with overall security governance being outside of the IT function. There is now a managerial qualification available for security managers. The Certified Information Security Manager (CISM) designation is available by examination from ISACA[2] and is targeted above the technical level of CISSP[3]. So my ideal

[1] Control Objectives for IT from the Information Systems Audit & Control Association (www.isaca.org).
[2] Information Systems Audit & Control Association.
[3] Certified Information Systems Security Professional.

organisation would be accredited to ISO 27001, have a CISM outside of IT and a couple of CISSPs within it to administer the processes defined by the Chief Security Officer. CMM level 5 is the way to go boys, so ascertain where you currently are and then initiate an improvement programme to close the gaps.

John is editor of BCS IRMA's award winning *Journal* and Managing Director of LHS Business Control, a corporate governance consultancy that he founded in 1988. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454.