Information Security Now - 2

John Mitchell

The old adage that those who can do, do and those who can't teach is often transferred to auditors. In some cases it is sadly true that the financial auditor is out of touch with reality, but in the case of IT auditing this is seldom the case and often they have the qualifications to prove it. Indeed, the CIO who challenges the auditors right to exist does so at his/her peril. The loaded question "so what are you're your qualifications for auditing me?" is often rebutted with, "Well, I am a Certified Information Systems Auditor, I hold an MBA where I majored in information systems control and I have a doctorate in risk management. What are your qualifications to run your IT department"? The turning of the tables with that last sentence is often so easy to do because only a small percentage of IT people are either academically or professionally qualified. In fact, this is more true of the older and usually higher placed people such as CIOs who may have vast experience, but this is not reflected in even membership of a related professional body, such as the BCS.

A few years ago I was down in Australia attending a conference where the CEO of a major bank stated that IT was a complete waste of money. What he was actually doing was venting his frustration that the ever increasing cost of IT never seemed to really justify the huge investments he was required to sign-off. As this was an IT conference and his CIO was in the audience, I tracked the latter down (in the bar naturally) and asked him what he thought of his CEO's comments. He responded that he was bitterly disappointed with the comments, that he and his team worked their socks of for the company and never received any recognition, etc, etc. (I have loosely translated this from the Australian that we were communicating in). I asked him why he hadn't done a straight forward cost-benefit analysis to show his boss the contribution that IT was making to the bank? In fact, the phrases "IT governance" and "balanced score card" inadvertently slipped from my lips. He responded that he didn't have time for all "this MBA stuff", but relented somewhat when I asked him to play a game with me along the lines of "if the bank didn't have any IT what would it need in the way of resources to provide the level of service it currently provided to its customers". It didn't take long to identify absolutely huge staffing, accommodation and other costs which far outstripped the IT budget and he howled at the end "and they still couldn't provide a 24x7 five second response time to a customer in their home". I left him a far less depressed person than when I had found him and with a conviction that maybe a little learning was not such a bad thing.

The best IT auditors will be at least CISA (Certified Information Systems Auditor) qualified. This examination is difficult to pass (the current pass rate throughout the world is only 52%), but over 40,000 people hold the right to use the designatory letters. Now simply passing the exam does not give you the right to use "CISA" after your name. You have to prove that you also have five years IT auditing experience and to retain the right to use the designation you have to prove an average of 40 hours per year of continuous professional education. This latter is one of the toughest of the CPE requirements of any organisation and is to ensure that the holders of the CISA designation remain

up-to-date. I passed my CISA in 1986; the days of mainframe computers and dumb terminals. Without the CPE requirement I would still be stuck in the dark ages of IT auditing, whereas I am often more current than my IT colleagues.

What has this to do with computer security I hear you ask? Well, the organisation that moderates the CISA qualification is the Information Systems Audit and Control Association[1] (ISACA) which also offers a qualification in IS security management. Its Certified Information Security Manager (CISM) offering has the same stringent requirements of its CISA cousin, but is aimed at IS security managers. In hierarchical terms it stands above the CISSP (Certified Information Systems Security Professional) in that it targets managers, rather than security officers. Many IS auditors also hold CISM too, so they can answer your opening question with both barrels of their weaponry. ISACA also provides, through its sister institute the IT Governance Institute[2] (ITGI), Control Objectives for IT and Related Technologies (CobiT) which is used by both CISAs and CISMs to provide a co-ordinated approach to implementing and measuring IT Governance in an enterprise. ISACA's research investment is huge and much of it is invested in enhancing CobiT to meet the demand of today's regulatory environment. CobiT has been mapped against all the relevant IT standards so a CISA qualified auditor will not be frightened by the fact that you use ITIL and likewise a CISM will not bat an eyelid when you claim to be aligned with ISO 27001. You had just better be sure that you are though, because any gaps will be quickly identified by the tools available to these people. Qualified IT auditors and security managers have a large toolset available to them which makes PRINCE 2 look lightweight. This provides a consistent approach in either implementing IT governance or providing assurance that it is at an appropriate level for the enterprise concerned. As IT security management is simply a sub-set of IT governance you need to have the former in place to achieve the latter. CobiT allows you to measure your process maturity using the CMM methodology first proposed by Carnegie Mellon university for software development. CobiT has expanded this to measure the maturity of 34 key IT processes. Not a bad starting point in showing how good, or how bad your IT department is. So be careful when you challenge an IT auditor on their ability. You may find that both their weaponry and their armour is bigger and tougher than yours.

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.

[1] www.isaca.org
[2] www.itgi.org