Information Security Now - 14

John Mitchell

It's that time of the year when we try to crystal-gaze into the coming year. In the financial columns the journalists are hung out to dry on their previous guesses as to what was going to happen in the current year, but us IT governance, security and assurance specialists usually get way scot free because we are smart enough not to try to predict the unknowable. However, as this is December 2009 and the editor has requested, asked, nay demanded that as an assurance provider (auditor in real speak) I must provide said prediction I will attempt to fulfill my duty. I have previously written that "we can control the technology pretty absolutely, but we can only manage the people" and that is my prediction for 2010. We will continue to tie down the technology and we will expand its ability to protect us from wayward humanity by preventing attacks while enhancing its monitoring capability to detect misuse of the technology. The mantra of "confidentiality, integrity and availability" will be expanded to embrace "compliance". Compliance not just with statutory and regulatory requirements, but also with international standards and best practice. Organisations are now approaching me with requests as to how they can enhance their IT governance, whereas until very recently I was hammering on their doors trying to obtain admittance. Why this change in behaviour? First, there is growing recognition that it is humans that are the risky component and as they can only be managed you need to have a suitable governance structure which recognises and manages the key risks. Trust is no longer an option as a control mechanism. Something stronger has to be put in its place which brings me to the main international standards for IT. ISO 38500 for IT governance, ISO 20000 for service delivery, ISO 27000 for information security and ISO 9126 for software quality. Wrap these up with ISO 9000 for quality assurance and you have a pretty bullet proof IT function. If you then adopt best operational practices from Control Objectives for IT (CobiT) and value for money concepts from Val IT you can prove your governance maturity to anyone who asks. These two products from the Information Systems Audit & Control Association (SACA) and the IT Governance Institute (ITGI) respectively provide a wealth of information on the control and management of IT and its associated people. Security is a sub-set of governance and I visualise the security professionals embracing the governance concept as a way of both expanding their power base and protecting their rear ends. The use of metrics to show that their protection and monitoring mechanisms are both effective and providing value for money will become a standard part of their toolset. After all, Sir Robert Peel said that the measure of a good police force was the absence of crime so it can be argued that the measure of good security is the absence of security breaches; especially if other organisations are experiencing an increase in security events. Now, you cannot collect these metrics without knowing what to collect which is where the risk governance framework comes into play. I can hear your groans now, but there is a direct correlation between good risk management and governance maturity. Basically if residual risk is low, because of good control, then governance maturity is high. I can measure the governance maturity of any IT function in just a few days by examining its relative maturity across 34 key IT processes. The difficult part for the IT function is deciding how it then goes about improving its maturity in selected processes. They get depressed when I show them that their change management process is based on a trust model. Remember the audit motto: trust but verify. True for governance too. And when did you last find a security professional who trusted anyone? So here are my predictions for 2010 and these are threats to the security manager. Less trust in trust. More trust in using standards and best practices. More metrics to prove that the governance model is effectively operating. More reliance on the technology and less on people. But as the technology is designed by people there will be a rise in the need for suitably qualified security managers. What qualification? Well, there is only one candidate here. The Certified Information Security Manager (CISM) from ISACA. CISSP is fine for the security administrator, but I am talking high-level security governance. Sorry, but that's the way the game is going.

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