Information Security Now - 23

John Mitchell

I received a letter from a company encouraging me to register for their on-line service. It included the instruction to change the password provided by them to one that was six to eight characters long, containing at least one upper case letter, one number and a special character. When I attempted to log-on I was asked for the second and sixth character of the password. At that stage I gave up and wrote it down. Sometimes the security gurus drive us to dysfunctional behaviour by the complications of the mechanism they design, but at least their heart is in the right place. On the other hand we sometimes get things that serve no real purpose, such as the annoying information on another site which tells me how long I have been logged-in. In the context of that site the information I really require is when I last logged-in, as that will alert me to unauthorised access. Telling me that I have been logged-in for five minutes serves no useful purpose. The security mechanism needs to be contextual and aligned with the required level of protection. Which raises the issue of security governance. This is a top-down approach which initially requires the identification of the risk and value drivers associated with the overall security requirements of the enterprise. Security costs money so the Chief Security Officer (CSO) needs to be adept at calculating the benefits (potential savings) arising from having good security as well as the associated costs. Costs, both direct and indirect, are easy to calculate, but the benefits equation is a bit more tricky. What value should be assigned to loss of goodwill, for example? Security is a mix of technical and human issues. The technology is the easy bit. I have never known a technology asset to deliberately defraud, or attack me without human help. We cannot control people, we can only manage them and this is where security governance comes to the fore. We create the organisational structure, leadership, training, tools, policies, standards and procedures to protect our information assets. Always being cognisant that the technical people are our greatest threat. After all, we have given them the training, tools and privileges to create the security infrastructure so it is not too surprising that they are our greatest threat. Nowhere is this more obvious that in the change management process where there is a heavy reliance on both technology and trust. The latter is the weak area as trust is not a control mechanism. The reason why we have segregation of responsibilities is to remove trust from the control equation. So the first security governance question has to deal with any areas where opportunity, ability and access to assets come together. The usual management response is that there has never previously been a problem in that area (that they know of). My response is that I haven't died yet, but it may just happen tomorrow. Ultimately, if security is a human issue, then perhaps we need to examine the position of the CSO in the organisational structure. I would leave the various security administrators within IT, but I believe that the CSO should be placed elsewhere. For years I have argued, with only moderate success, for the CSO to either report directly to the Chief Operations Officer (COO), or to the head of human resources where the enterprise does not have a COO. This helps with segregation of duties and brings a business perspective to security which is sometimes lacking when the CSO is part of IT. The business perspective is all important when it

comes to calculating the cost-benefit equation, which is why you need someone with a wider perspective than is usually found from within the narrow technical confines of IT. So the CSO needs to understand both the business and the supporting technology. In comic book terms we are talking of someone who wears their underpants outside of there trousers, wears a cape, has abnormal strength, flies through the air and has a big letter S on their front. These super people should be able to bridge the gap between the business and the technology and as a result realise the dangers associated with end-user-computing (EUC) where technology is integral to the business product. Indeed, EUC is one of the most risky (and beneficial) aspects of computing, but it often receives the least oversight from the CSO. Perhaps it is a case of out of site is out of mind? Which is understandable, but not from an overall security governance perspective; especially when the FSA is handing out large fines for incorrect spreadsheets and the ICO is doing a similar thing for poor personal data management. The CSO must look beyond the technology, but be able to manage it via his security administrators and more importantly, from a business perspective.

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of Council and current chair of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)1707 851454