Information Security Now - 13

John Mitchell

Organizations spend millions defending their cyber perimeters, but only a fraction of that in protecting themselves from insider threats. This is despite all the evidence pointing to insider threats as being a significant risk area. We train our staff (and contractors) provide them with the necessary privileges to do their jobs and then we basically forget to monitor them. Where we do monitor it tends to be either spasmodic, or superficial, or both. I was once told by a Chief Information Officer (CIO) that “we have trust someone” and when I asked why he was reduced to incoherent spluttering. The audit motto by the way is “trust, but verify”. I was once involved in a job which required us to check a network to detect undesirable images. I discussed it with the CIO and explained that first we would tell everyone of our intentions and then we would do the actual check. My logic being that the advance warning would see an immediate deletion of the embarrassing items. Lo and behold that was exactly what happened and the company recovered about twenty percent of its total disk capacity without firing a shot. However, I was amazed to find that when we did the subsequent check the only real offender was the CIO himself. At his dismissal hearing I asked why he hadn’t taken advantage of the warning. His response was that it never occurred to him that we would check his files. A strange, but not a totally unexpected, response from a senior manager. I once has to deal with a Chief Executive who shared his access credentials with his secretary despite this being a dismissible offence. His response was similar to the CIO’s; the policy did not apply to him. We can control the technology pretty absolutely, but we can only manage the people, but control and management are not quite the same thing. We manage people by implementing policies, standards and procedures, but until we can implant a controlling chip (which is what most governments would probably like) we are still unable to control them. It’s not the computer that steals the money, but the person. It’s not the computer that causes the data leak, but the person. A computer does not carry out a denial of service attack unless subverted by a person. That abnormal program termination is caused by the programmer, not the program. The covering of tracks by deleting a log file is person inspired and not the idea of the computer. So people management is really important. Actually, it is quite critical and that is one reason why I have argued, quite unsuccessfully for some years, that security is a human resource challenge. After all, it is HR that conducts the initial background check. It is HR that sets the employment policies and staff review processes and it is HR that drives the termination process. All in all, it is a pretty solid case for HR driving security. Indeed, perhaps the chief security officer (CSO) should be part of HR? I am aware that neither HR, nor IT, are happy with this idea, but there is no doubt in the mind of the International Standards Organisation that information security is a corporate and not an IT responsibility. Currently, information security tends to be driven by IT and the CSO is usually an IT professional who would see his career prospects severely limited if he were part of HR. Likewise, the HR professionals see technology as an IT responsibility and do not have the necessary knowledge, or inclination to get involved. However, if information is a corporate responsibility, then it stands to reason that information security should be integrated into the business processes (maturity level 5 for those who read my last article) with a much enhanced prospect of preventing and detecting insider threats. It may seem strange, but technology security is really a people problem. A soft problem, rather than a hard technological one. People are the soft underbelly of the enterprise and the role of HR is to ensure that processes are in place to manage them. Hence information security is really an HR challenge. How else can you manage that systems administrator who you have just provided with super user status?

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