Information Security Now - 25

John Mitchell

I have never yet been defrauded, or attacked by a computer of its own volition. There has always been some guiding human influence. The reason for this is quite straight forward for although we can ***control*** the technology absolutely, we can only ***manage*** the human component. This is because, until the government starts chipping us at birth, we have free will, whereas the technology does not. We attempt to manage the human side of IT by a hierarchy of policies, standards and procedure, but the human can choose whether, or not, he will follow the rules. A good person can make a poor system work and conversely a bad person can make a good process fail. I have long argued that the place for a security manager is within HR, rather than IT. My arguments for this being that HR is our first-line of defence against recruiting bad, or incompetent people, which it does by verifying academic and professional competencies and following-up previous employment claims. They are also our second-line of defence in that, hopefully, they ensure that the correct IT privileges are allocated for the role(s) that the new person will fulfil. They also provide a third-line of defence through the regular appraisal process which will hopefully detect signs of people deviating from the straight and narrow. Finally, it is HR that manages the termination process which (again hopefully) removes the IT privileges that were previously granted. So HR are an essential management component in securing the human in the employment life-cycle. However, and there is always an however for us auditors, we must also consider the evidence from various research projects which show, with remarkable consistency, that twenty-five percent of a given population are totally honest, another twenty-five percent are basically dishonest with the remaining fifty percent being only as honest as the system under which they operate require them to be. Thus, if we have well managed and controlled operations we keep seventy-five percent of our stakeholders honest, but if they consider our controls to be weak, then the converse is the case. Preventing someone abusing a process where they have been granted them specific privileges is very difficult. For example, if I am a refund clerk I can provide refunds up to my limit to anyone I like. Likewise, if I am a programmer I cannot be prevented from inserting malicious code under the guise of an authorised change as I have the privilege of amending code. The likelihood of detection is therefore a key element in determining whether, or not, I will attempt to abuse the privileges which I have been allocated. If I consider the detection element to be strong, then as one of the fifty percent ‘undecided’ on the honesty front I will err towards the honesty side, whereas if I consider the likelihood of detection to be poor, then I am more likely to attempt something dishonest. We can consider this in the more technically challenging IT jobs such as systems programmer, or network administrator, where we have very skilled and intelligent people who are aware of the efficacy, or otherwise, of the control environment, as they were probably involved in constructing it. Securing these people is indeed a challenge, but not totally impossible. A little bit of divide and rule (segregation of duties) can go a long way, which is why us auditors are always interested in organisation charts, job descriptions and privilege allocation. Risk management is an important part of securing the human which is why we have endless debates as to just how many super users

you really need and then how those users are to be managed. Systems staff are high risk individuals so far as the company is concerned. They are provided with powerful privileges and then we rely on trust as our control mechanism. However, trust is not a control. This is not just an academic exercise. Why do you need two people to launch a nuclear missile and why are the launch stations several yards apart? The answer is obvious. You do not want one person with the ultimate power to start Armageddon on their own. Likewise with the key IT positions. Obviously, collusion will overcome the best of controls, but that is the challenge of securing the human. You always hope that one of the parties will either fall into the twenty-five percent honesty bracket, or that they will be so frightened of being caught that they remain honest even when the opportunity arises not to be so. Ultimately, we can ***control*** the technological privileges we allocate, but we can only ***manage*** how they are used.

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