Information Security Now - 20

John Mitchell

Being a computer auditor my job, like many others, has both primary and secondary roles. My primary role is to provide assurance, or otherwise, to management that the CIO is adequately managing his/her risks in order to meet their business objectives. My secondary role is to help in the design of business applications so that when they enter production they will be suitably controlled. Being a Certified Fraud Examiner (CFE) I also have a tertiary role for conducting special investigations; particularly in the area of cyber crime. Now I do not want to get too legalistic on this as I am not a lawyer, but to my mind cyber crime is committed by individuals, or groups, whereas cyber warfare is committed by governments. Does it matter? Not from a cyber defence point of view perhaps, but rather from the way it is played and the end-game. Dealing with cyber crime within a legal and regulatory framework means that there are six potential end-game scenarios depending on whether it is as a result of either an internal, or external attack. These are discipline, resignation, dismissal, civil prosecution, criminal prosecution, or make it go away. Although the last one may be viewed as morally wrong it is often the easiest and cheapest from a company perspective. Whichever route is chosen, or imposed, the rules are defined and the operating parameters and constraints are usually quite clear. With cyber warfare there are only two possible outcomes, victory or defeat and the constraints are pretty much unlimited. There is no Geneva convention to define what is, or what is not allowed. So the concept of total cyber war is equivalent to blanket bombing. Hit everything and there is a good chance that you twill ake out something important. But here resides the problem. We know that blanket bombing is only effective against the civilian assets. The military ones are usually too well protected to be harmed as the Allies found out in World War II and the Americans in Vietnam. Likewise, with cyber warfare it is easy to take out the civilian assets, but no so easy to destroy the military ones. However, if the military are dependant on the civilian infrastructure, then taking out the infrastructure renders the military assets isolated. The second world war was very much won because the Allies had superior intelligence and used disinformation as an attack mechanism. D-Day was not so much won by the Allies, but rather it was lost by the Nazi's, because they relied on disinformation from agent Gabo. To the extent, that even two months after the initial landings they were still convinced that Normandy was just a feint and so they held their reserves to repeal an attack on the Pas de Calais. Perhaps we can learn from this? If the next wars are to be won by the side with the fastest computers (overwhelming strength is still a huge factor in warfare), then perhaps the only way for the weaker side to survive will be by the use of intelligence coupled with disinformation. If we can predict where the attacks are likely to come from (which countries are turning out the most computer science graduates?) then perhaps we can limit their capability by destroying their sites at source? The equivalent of hitting the V2 sites before the missiles could be launched. The equivalent of a pre-emptive strike. On the disinformation side we can create "honey pots" as targets. As cyber war is unlikely to be declared in any meaningful way, we need to be prepared for a devastating and overwhelming attack on our critical computer assets. The

people responsible for our critical national infrastructure only have an advisory role as was disclosed in a response to an enquiry from me regarding the nations electricity supply, which I quote in full. "*CPNI provides protective security advice to the businesses and organisations that make up the national infrastructure in order to protect against terrorism and other threats to national security. Advice is targeted primarily at the critical elements of the national infrastructure, which includes the UK's electricity supply industry. The nature of the advice that we give is discreet between CPNI and the receiving entity and therefore we are unable to provide further information in response to your question*". Any actions taken by a company based on the CPNI's confidential advice is likely to be based on the commercial considerations of an individual company. Our electrical infrastructure is provided by several companies which are in competition with each other, so getting a consensus to help the nation as a whole is an interesting concept. Capitalism is primarily selfish so what is the incentive for any company to incur costs which do not benefit its own investors? Indeed, it could be held that the directors are acting illegally if they are doing things that are not of direct benefit to their shareholders. Likewise with our computer infrastructure, but perhaps its very diversity is our protection which is how I now return to my job as a computer auditor. Service availability is the name of the game, with an almost universal requirement for a 24 x 7 service to those who should receive it at the time and place of need. My job is to ascertain whether the risks associated with this requirement are being adequately managed. The key word here is "adequately". A very granular concept. What is adequate for a charity may be not be adequate for a bank and what is adequate for a bank may not be adequate for a nuclear power station. Change is an ideal time to insert a devastating Trojan under the guise of an authorised change. The majority of my clients have a huge vulnerability in their change management process which tends to be "trust" based. The audit motto is "trust, but verify", which in reality means that we only trust after it can be proved that the trust is justified. Something the Nazi's should have taken on board before they believed Gabo and held their reserves back at D-Day.

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of Council 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 on +44 (0)1707 851454