Information Security Now - 17

John Mitchell

I started my last column along the lines that ARPANET, the predecessor to the Internet, was designed to survive an atomic war. On of my readers (assuming that I have more than one) has pointed out that this is an urban myth, for which I apologise, but it did get me thinking about separating myth from reality. Anyone who has read Stieg Larsson's Millennium trilogy will know about a group of fictional hackers who can target the computers of undesirable elements at will. Nothing can prevent them from breaching even the best of protection systems. However, this group of hackers have a huge advantage over the rest of us. They know who their enemy is and where in cyberspace he resides. My company's server is constantly being "pinged" to ascertain if there is a live computer at that particular internet address. We know through using tracing software that the majority of these queries appear to come from two universities: one in Europe and the other on the Indian sub-continent. I use the word "appear" simply because we don't know whether these universities are unknowing conduits from another downstream source, or whether the address we see is a spoof. Not knowing your enemy is unnerving, but as our firewall does not respond to the pings they don't know about us either. In much the same manner that naval submarines operate in stealth mode we tend to do the same, which is why I have never bothered to contact the administrators at the universities concerned. To do so may reveal our existence to a potential enemy if it is the administrators themselves who are conducting the reconnaissance. Our firewall neutralises their pings, our anti-spam filters limit the amount of junk mail we receive, our anti-spyware protects us from Trojans and the anti-virus software keeps us safe from infection. In much the same way that the alien in the film Predator was invisible and could only be seen indirectly, we have the same challenge with the black-hat hackers. I mentioned that we had traced the pings against our firewall to a couple of universities, but all we really know is that someone out there is sniffing around. Who, and ultimately from where, remains a mystery, which is one of the problems associated with taking away people's internet access if they are deemed to be illegally downloading copyright material. Is it really them? So we offer passive resistance to an unknown enemy. But isn't attack sometimes the best means of defence? Oh to be able to attack them, but two things make this very, very difficult. The first is that we don't know who they are and the second is that we are law abiding. The UK's Computer Misuse Act makes it impossible to conduct offensive action and remain within the law. My passive defensive stuff is okay, but any move into offensive action could result in me spending up to ten years as a guest at Her Majesty's pleasure. So in practice I am dependant on the Government to take the necessary action. The thought of a cyber 007 slipping silently into the spammer's base, wrecking their systems and just as silently departing is comforting, but naïve, so I have to rely on commercial products to defend myself and hope that there are secretive white-hats out there who are taking the battle to the enemy. High-tech Zorros who identify and destroy the enemy. Well, if this happening they appear to be losing the fight. Simply having right on your side is no protection against thirteen year old kids who subvert hundreds of computers and are then able to carry out distributed denial of service attacks

against individuals, organisations and even governments. Only when the latter suffer a really severe disruption will they start to take things seriously. Interestingly, the Americans have a cyber warfare school, but they still find themselves wide open to a hacker from the UK seeking information on aliens. If Gary McKinnon was able to break into those ninety-seven military computers and if he was able to do the $800,000 damage claimed, then the world's only superpower has pretty much wasted the last ten years of its much publicised cyber warfare capability. Electronic warfare is cheap, can be launched from anywhere and leaves little in the way of hard evidence. The unknown enemy, operating from an unknown base who can strike at the speed of light. The Chinese supposedly have 100,000 people researching and developing cyber warfare techniques. In May this year the Americans created a "Cyber Command" within their Department of Defence with a total staffing of around 90,000. We have a few dozen. Size may not be everything and quality is the prime requirement, but statistically you are bound to have more quality people in a large population than from a small one. If you are not worried by this, then you don't really understand the problem and if you don't understand the problem, then to quote Malcolm Forbes, "it's so much easier to suggest solutions when you don't know too much about the problem". On balance I prefer the George Orwell quotation that "people sleep peaceably in their beds at night only because rough men stand ready to do violence on their behalf".

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is 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