Information Security Now – 27

A few months ago I read an article from a technology journalist regarding the hijacking of his Apple iCloud account and the subsequent deletion of all the data on his iPhone and other devices. Note, it was the hypervisor that had been hijacked and not the device which provided the back-door into his phone. This leads to all sorts of concerns over the security of mobile devices. Many of us will have loaded software to enable us find our phone if it is lost, or stolen, and to remotely delete the data held on it at our instruction, but in this case the attack came from above rather than below which raises the game somewhat. Instead of tackling the risk associated with an individual device we now have the nightmare scenario of all of a particular mobile breed being threatened in the mass. A few years ago Amazon remotely deleted a number of books from its customers' Kindle devices on the basis that the books were 'unauthorised', but such was the outcry they stated that they would never do so again. However, Amazon's terms of use state, 'all content included in or made available through any Amazon Service, such as text, graphics, logos, button icons, images, audio clips, digital downloads, and data compilations is the property of Amazon or its content suppliers and protected by United States and international copyright laws'. So you do not own the book, you have only paid for a conditional licence to it and Amazon can take that away any time it likes. With devices linking to the Internet via Bluetooth and Wi-Fi you can just as easily be presented with a wipe command rather than a book. Ditto for any of our phones, tablets, satnav and anything else which receives updates from the sky. The current view on cyber war is that it will involve attacks on servers, but why attack the hardened server when you can go for the less well protected node? Especially if you can get to them simultaneously from the sky. We now have the potential to conduct a reverse Distributed Denial of Service Attack (rDDoS). Instead of many devices attacking one, we have a single device able to attack the many. Take away the access points and the hardened central device becomes useless. Which reminds me of those debates regarding service availability. Where do you measure it from? The central server, or the user's access point? The technology boys always wanted the former as it was under their direct control. The users always wanted the latter because that was where they received the service. Taking my argument regarding a reverse DDoS attack we can see that having a fully functional server is useless if all its access points are disabled. So I think that the users were correct in asking for the service to be measured at point of receipt. Even more so now when the absence of a signal can render our investment in the technology worthless. Worse still if all of our files and documents are held in the Cloud and accessed by our mobile device with no local copies to fall-back on. When we moved from batch computing to real-time we dramatically changed the control paradigm for the worse and it has taken us ages to catch-up. Not that we really have caught-up, but at least we can (hopefully) explain the risks so that management can make reasonably sensible decisions. Now the control paradigm has changed again and we are basically back at level one on the Capability Maturity Model (CMM)[1] scale, which is pretty much as bad as it can get. The military equivalent of giving a soldier a rifle, but withholding the ammunition from him, although in such a case he can still use the weapon to club the enemy to death.

[1] 1=initial & ad-hoc, 2=repeatable, 3=defined process, 4=managed & measured, 5=optimized

All military aircraft have GPS, but in the event of the GPS becoming unavailable they fall-back to inertial guidance systems based around spinning gyroscopes. What fall-back do we have if our access points are removed? It is often claimed that the next war will be won by the side with the fastest computers. I am not so sure. Without our access points we will be unable to use our powerful IT assets and will be totally helpless in the event of a reverse DDoS attack. Mobile devices may currently be our greatest benefactors, but without some form of fall-back they may well become our greatest foes.

John Mitchell

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