Information Security Now – 36

Do you remember the Osborne luggable? Not if you were born after 1980 you wouldn’t. This was one of the first portable computers, if you consider carrying a 10.7 kilogram sewing machine around as defining portable, but it was the start of an era. The Osborne led to the laptops we know today which in turn lead to our smart(ish) phones. Now we have wearability in the form of smart watches and intelligent clothing. Mobile computing has never been cheaper or easier than it is today. Connectivity is provided by the cell phone system, Wi-Fi hotspots and in some instances by direct satellite connections. We can print directly to our 3D printer on the other side of the world, switch on our car’s air conditioning ready for the commute home and set our home central heating up a notch on the same journey. Our clothes can monitor our heart and temperature and report the results directly to our medical monitoring system. I can log into my corporate server from anywhere in, or off-world, and conduct conference calls on the move. However, and there is always an ‘however’ when dealing with us assurance professionals, the above are totally dependent on network availability. Without the network the internet of things are just separate pieces of junk with no real capability in themselves. No matter how portables these devices are they depend on the invisible thread of the network service to fulfill their potential. Availability is one of the cornerstones of the confidentiality, integrity and availability triangle and without it the other two are basically meaningless. When the bombers hit London on the 7th July 2005 the security services switched-off the cell phone network to prevent the possibility of bombs being triggered by cell phones. Chaos reigned as a result of this action because most disaster recovery plans rely on a notification list which, in the majority of cases, comprised cell phone numbers. No network, no availability, no workable plan. Thousands of people evacuated from their offices were pushed north, west and east (south was not an option due to the bridges across the river Thames being closed) without any real idea as to what was going on as they were without the means to communicate, such had become their dependency on the network. Russia removed Estonia from the web in 2007 amid that country's disagreement with Russia about the relocation of the Bronze Soldier of Tallinn. This was predominately a DDos attack, but the result is similar to the loss of a network; non-availability of a service. So the first risk associated with mobile computing is the loss of the communications mechanism.

The second significant risk is the dichotomy of the first; the availability of the service to a non-authorised person, or persons. Some ten thousand cell phones are simply lost on the London transport system each year, while six thousand laptops are misplaced in London taxi cabs. If any of these are connected to the corporate database at time of loss, then the finder has the potential to use that connectivity as they are effectively the person who lost the device, with all the associated privileges of that person. Even a one-time password generator offers no protection as the session has already started. Couple this with the easy way by which Wi-Fi networks can be hijacked and even security conscious, but busy executives may be tempted to use the coffee shop’s free network whilst they sup their cappuccino. When I went with my wife and her friend to view the Sea of Blood at the Tower of London they both wanted to purchase a poppy. The gift shop said that we had to order on-line and could use their free Wi-Fi network to do so, as there were only a few dozen of the poppies left. I declined to do so, much to the annoyance of my wife (really dangerous thing to do) as I explained that I was not sending our credit card details over an unknown network. Once home, I placed the order and obtained the last ten poppies available. That was a narrow squeak, as I probably would not be here now if they had all been sold. So, one can avoid being defrauded over the internet, by not using the internet, but one would lose many opportunities. Likewise with mobile computing. The risk of a loss versus the opportunity of a gain. If you know the risks and effectively manage them, then you are totally aware of your risk appetite. With mobile computing non-availability versus incorrect availability and this is before we even consider the confidentiality, integrity and compliance aspects. Over to my security colleagues?

John Mitchell

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of BCS Council and 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)7774 145638