Information Security Now – 28

One of my favourite films is *Invasion of the Body Snatchers* where the population of a town is replaced by emotionless alien duplicates. The reason that I like it is because it raises the question, in quite a thoughtful way, of how do you tell the real person from the duplicate? Which is the very problem faced by users of social media sites. How do you know that the person you are communicating with is really them and how would you know if there is a clone of you out there, either circulating slanderous allegations about a public figure, or obtaining loans under the guise of your profile? In essence how do I know that you are you and how do I know that I am me? The drive-by collection of Wi-Fi traffic by Google as part of its Street View programme not only caused public indignation, but also resulted in financial sanctions on the company. Google claimed that the data collection was caused by an overenthusiastic engineer who had inserted the relevant code without authorisation (which raises concern about their change management process) and that no use was made of the collected information. Although this security breach was not social engineering in the accepted sense, it did reveal that many people had inadequate security over their wireless traffic. It takes little imagination to believe that these are also the very people who give away their personal data for free via the various social networking sites. Most of the security on these sites relies on the old user identification and password combination coupled with self-service password reset in the event of a forgotten password. Password resetting is usually a challenge-response process based on pre-set questions and answers and this is where the security equation breaks down, as the answers to the various questions are usually in the social networking public domain such as: mother's maiden name, birthday, first school or job, pet's name, etc. Other information provided may be used to ascertain if someone is on holiday and therefore their home is available for an out-of-hours visit. Identity theft is aided by the plethora of information freely provided, coupled with the ease of downloading logos and identity card formats from the web. As part of a fraud investigation that I was involved in, the police stopped a suspect's car and found over thirty sets of identification: passports, driving licences, bank statements, etc. It turned out that the suspects full-time 'job' was to travel between the various benefits offices claiming for the benefits of the false identities. He retained twenty-percent of the proceeds (his wages) and passed on the rest to his controller. A few years ago my younger brother started receiving threatening letters from a bank (not his) regarding missing repayments on a £10,000 loan he had supposedly taken out with them. A visit to the branch (with suitable proof of identification), revealed photo copies of a his driving licence, passport, bank statement, utility bills, etc., plus my brother's apparent signature on the loan agreement. The only real discrepancy was the date on the agreement which clashed with my brother being out of the country. The bank was adamant that it was my brother who had attended with the relevant information, although they had to confess that the manager who had dealt with the application had since left the bank. I noticed the existence of CCTV and asked for how long they kept the recordings. The time-frame was within that of the loan application, but my request to view them for the date concerned was refused. After some tussle it was agreed that the bank's security staff would do so. A few weeks later we were informed that the bank would be taking no further action and that my brother's credit record would be updated accordingly. To this day we have no

idea how the fraudster (probably the loan manager), got copies of the various documents. My brother is an enthusiastic social networker, but to his knowledge he had never uploaded images of his driving licence, or passport. However, copies of these had been taken over the years for various other proofs of identity, so we assume that there is a trade in such items. I then went through what personal data items my brother had revealed on his various social sites and was able to create a very accurate profile of my brother's business and social life and certainly sufficient to masquerade as him and to gain access to his various media accounts; especially after simulating the theft of his unprotected mobile phone and copying the data. As some 10,000 phones are simply lost on the London transport system each year and as the statistics indicate that a large proportion of them are unprotected, then the potential theft of personal information for other manipulation is huge. In the climax of *Invasion of the Body Snatchers* the heroine is no longer certain the her hero is really he. Likewise with social media today. So me becoming you may not only be nearer than you think, but may already have happened.

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