Information Security Now - 18

John Mitchell

For some fifty minutes recently our American cousins lost communication with around seventy of their nuclear tipped missiles. Russia has previously taken Estonia off-line and the text to my Nokia cell phone was brief, but informative. “Your mobile has won £415,000 (Nokia UK Promo) Payment no. MK357. For claims email claim@nokiauk.uk.co.uk & call +44 704 5774 118”. I know that I should be more concerned with the two previous threats, but this one was closer to home. The email address looked decidedly dodgy and when I checked the sender’s number is was from Ghana. So my get rich quick hopes were once again squashed, just has they had previously been in relation to the nice man from Nigeria who wanted my help in moving USD $40 million out his country for which I would receive a USD $5 million commission for my time, my bank account details and a letter of authority. The interesting thing about all of these scams in that they rely on three common things to be successful: greed, gullibility and technology. It is the last one which enables the scammers to operate remotely, hit large potential audiences and put forward any persona that they believe will tempt you. Whereas you may have concerns about the integrity of an unwashed, unshaven person wearing a yak coat and carrying a Kalashnikov, these may be somewhat allayed if you see a photograph of a business man in a smart suit sitting in an office. Even respectable businesses are not adverse to using a little technology to steal our electronic assets, as was revealed when Google reluctantly owned up that their Street View vehicles were (inadvertently) collecting details of Wi-Fi networks as they cruised by. Not so much a drive-by shooting, as a drive-by looting. Now whatever the intent, and in my time I have dealt with intentions ranging from the most laudable to the most base, the fact that we can be robbed remotely means that we have to think wider than the locks on our doors. I recently advised a client who was based in a shared tenancy building that he certainly couldn’t rely on door locks as the outsourced cleaning company had free access to the building overnight. So on top of the logical security we built a CCTV recording system with motion sensors, off-site transmission of any triggered recordings and SMS alerts. It didn’t cost a bundle although the warning signs and legal advice were almost the biggest budget item. Did the signs have to be in languages other than English, for example? The system was operational before this was sorted and the Chief Security Officer had a few busy and heart stopping days while the system was bedding-in and he watched the cleaners systematically opening any unlocked cupboard, or drawer. Curiosity killed the preverbal the cat and it certainly killed the cleaning contract when he drew this to the attention of his CEO. Despite the lawyers saying that evidence collected covertly was likely to be inadmissible in court the CEO was not intimidated and the contract was cancelled. So although the electronic threats should not be ignored we need to remember that our secrets may be just as vulnerable from a physical threat. Security in depth is what I desire when I am asked to provide assurance that things are okay, but as we all know a chain is only as strong as its weakest link. I have a pseudo-mathematical technique for measuring control effectiveness, which although not perfect does remove some of the judgemental errors in reaching a conclusion. On balance I find that most control systems are based on trust and optimism, rather than hard-nosed pragmatism. The trust mechanism is usually there out of an unwillingness to face the reality that if you take trust out of the equation, then most control processes are pretty useless. I rely on my security officer colleagues to identify the current and future threats and to suggest appropriate controls. I then sit down with them to evaluate the effectiveness of the proposed controls. Will this control manage the likelihood, or the consequence? Is it preventive, or detective? On a percentage effectiveness measure, where does it score? Where does it sit in the seven control classes proposed by Brewer & List[1]? They often retort that as the likelihood of a particular threat crystallising is low, then it doesn't matter too much if the control is weak. I answer that they may not as yet have suffered a heart attack, but it would be useful if they could detect the symptoms early enough to get to the hospital before a full cardiac arrest took place. So we kick the thing around a bit and find that even with our best intentions the residual risk remains stuck in the "amber" zone. But that is life. Not everything is "green". Even more so now that the threats and controls may no longer be under our direct control. Outsourcing and cloud computing, reliance on third-party security statements and lack of understanding mean that we are more vulnerable than every to changes in the use of technology. Providing that management are aware of and are willing to tolerate a risk at a particular level, then my job is done. Despite that, it is still the people risk that fascinates me. I have never known a computer to attack me of its own accord. Even those 70 million zombie hosts that are waiting out there still need a human hand to direct their attack.

[1] http://www.gammassl.co.uk/topics/time/