Information Security Now - 24

John Mitchell

Last week I received a text message informing me that I had won £240,000 in a Nokia competition. This sounded good as it came to my Nokia mobile, but also bad as I hadn't entered any such competition. As an IT assurance specialist I am cynical by nature, but I am always willing to engage in a bit of banter at the expense of the black hats, but when I checked the return number I noticed it was one of those that would have charged me a few pounds for the privilege so I declined to become engaged. Not to lucky was my neighbour, who willingly disclosed both his bank account and credit card details in exchange for a similar bit of social engineering. And there we have it. You do not need to be a technical genius to take money from a naïve correspondent. Surprisingly, human nature tends to err on the side of trust. I say "surprisingly" because it is quite a nasty universe out there and yet we tend to give the benefit of the doubt in the first instance which is what the black hats take advantage of. I notice that in most instances it is easier to avoid an unpalatable truth rather than face it head-on, which is why I am no longer surprised that, when I point out a flaw in an enterprise's control mechanism, I am told that "you have trust someone". I have never seek the logic in this, although I do admit that I have some close friends whom I would trust with my life. However, these are not people of whom I know nothing, or who are of recent and small acquaintance. My niece on the other hand claims to have five thousand Facebook "friends", but I suspect that she has far fewer friends that she would like to believe. I know of several people who would like to be LinkedIn with me, but I know them not so I keep my distance. Perhaps I miss many opportunities for business, or social advancement, but I do not feel incomplete, sad, or lacking in social engagement, which are all the things that the black hats are looking for to engage me in their nefarious activities. So am I safe? Only to an extent. I am not so technically competent as to be able to fully protect myself from a sophisticated technical attack and a denial of service would badly hurt me, so I cross my fingers and put my faith in my anti-virus and firewall software. So do my friends and colleges, but they have one flaw which is lacking in me - trust. I once found a very simple expenses fraud which had gone unnoticed for some years because the perpetrator was trusted. Now the motto of the assurance specialist is "trust but verify". You can get my trust, but only after I have verified that the trust is justified. I earlier mentioned that I have a few close friends whom I implicitly trust. A couple of them have previously saved my life, so I owe them something and trust is my payment in kind. I cannot think of any equivalent in my business context and my attempts at implementing IT governance in organisations indicates that far too many companies would rather avoid an unpalatable truth than face it directly. I am fascinated by the psychology of the black hats and am not aware of any detailed research in that area (please let me know of any), but if they follow the mind-set of the typical fraudster (and I am making no such claim), then arrogance combined with contempt for their victims (they deserved it) would be the par. But I have to be careful, or I may suffer the same fate as Steve Gibson the designer of firewalls, such as Zone Alarm. Gibson made the mistake of publicly denigrating the majority of hackers as "script kiddies". One of these "kiddies" took exception

and conducted a sophisticated denial of service attack against Gibson's company web site. Now Gibson knew how to defend himself, but ultimately he had to issue an apology in order to stop the attacks, which apparently originated from a thirteen year old boy. Almost all the commercial companies I deal with are woefully unprepared for a direct attack against their web sites, or internal networks. Defacing a home page may not do any real damage to the firm's ability to continue trading in the short-term, but it does send a message to stakeholders that the firm has poor security and perhaps should not be trusted with sensitive information. Reverse social engineering if you like. Using a technical attack to send a social message, rather than using social means to obtain the ability to conduct a technical attack. Have we come full circle?

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