Information Security Now - 26

John Mitchell

Not so long ago if an auditor (now we are ‘assurance professionals’) wanted to find out what was really going on in the IT department, (s)he would lurk anonymously by the coffee machine and evesdrop on the conversations that took place. Nothing like a dose of caffeine to loosen the tongue. Now a good assurance professional will talk to anyone, which is why one early grey morning in New York I met someone at a coffee machine, whom I took to be the janitor, for a company that my client was thinking of acquiring. I was early for my appointment with the CEO and spent an enjoyable half an hour with Joe dressed in his vest and cut-off jeans. During the conversation it became apparent that their rocket scientists had developed a new trading algorithm, which was the reason for the potential acquisition and Joe, who held some shares, was hopeful of making a killing. However, he also let slip that the development guys never backed-up their work. He seemed to know far too much about the IT function for a mere janitor so I was on my guard and careful to non-committaly respond as to why I was over from the UK. We parted on good terms (it always pays to be on good terms with the janitor) and I went back into reception which was now staffed, announced myself and that I had an appointment to see the CEO. Five minutes later I was shown into Joe’s office! We both had a chuckle at our respective attempts at the coffee machine to probe each other’s knowledge and he was fascinated that I had picked-up on the lack of back-up of the development stuff. He became very concerned when I pointed out that the main reason my client was thinking of acquiring his company was because of the value of the intellectual property (IP) invested in his software. That magic trading algorithm was a living entity which was constantly being refined by the rocket scientists in the development environment. In the event of a local disaster that IP could disappear in a puff of smoke. Implementing a back-up routine was readily accepted and my client acquired the company and Joe retired to Florida as a very rich man.. The reason I recount this story is that you can never be quite sure who you are talking to, or who else may be listening into your conversation, which is why I am still quite amazed at the things people discuss when they are using public transport, or on their cell phones, which brings me quite nicely to a couple of security threats which I perceive to be upon us.

.

The AppStore on my smartphone informed me that I had three updates awaiting my attention. What were these updates and what did I know about the underlying code? Being an IS auditor I am very aware that most entities change management systems are rubbish – and these are the internal processes which I can deconstruct at my leisure – but here I was dealing with an external process of which I knew nothing.   So here is my first upcoming threat. What do we know about the content of smart phone apps?   Currently there are nearly half a million apps available for smart phones and Apple recently announced that some 25 billion apps have been downloaded from their store. An app is an application. A program. A piece of software. If we were loading software onto a corporate device we would, hopefully, have stringent change management processes in place. Couple this with the dangers of ‘bring your own device' (BYOD) and we have a situation where we may have no idea as to what code we are potentially unleashing into our corporate network. Currently, everyone is concerned about Cloud computing, which is not unreasonable considering the clear and present danger it presents, but standard control procedures can do much to mitigate the dangers associated with it. However, BYOD coupled with non-existent app management potentially presents a far more serious danger to the enterprise. If we then couple this with the threats presented by nation states conducting cyber warfare, we have an Armageddon situation where someone, possibly unknowingly, with a malware app on his/her smart phone walks into your company, links into your network and the embedded Trojan does the rest. So what can we do about this? Knowing the problem is half the solution, but managing it is a whole lot more effort. Those of you who have previously dealt with auditors will know that we do nothing of an operational nature. We provide assurance, or otherwise, that the process is well managed and we will not taint our independence by dirtying our hands with real work. So when the editor said that the theme of today's issue of IS Now was emerging threats and how they could be managed, I was aghast. Surely I was not expected to provide a solution? That's way above my pay-grade (and competence). Just who does he think I am? However, perhaps I do have a partial solution to the BYOD and smart phone Apps combination which involves using another potentially dangerous emerging technology – the Cloud. Don't let me connect to your network. Keep me in the Cloud on the other side of your firewall. Share things with me via the Cloud and if you take anything from me put it through your firewall, anti-virus and malware protection mechanisms. Treat me as if I have the plaque, because I may just have it.

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