Information Security Now – 30

In February of this year, SC Magazine listed its top-ten security threats for 2013. They were: state-sponsored espionage; DDoS attacks; cloud migration; password management; sabotage; botnets; insider threat; mobility; internet; and privacy laws. The recent revelation from Edward Snowden (I am writing this in September), the US whistle blower, that the National Security Agency is routinely breaking encrypted messages using brute force techniques and that they have also liaised with commercial encryption suppliers to provide back-doors into their systems, indicate that SC Magazine was on-the-money regarding its predicted threats. As a result I now need to change a key component in one of my presentations dealing with digital signatures. For the record, my main 2013 concerns were cloud computing coupled with Bring Your Own Device.

With 2014 coming along your editor has once again put us pundits on the spot by asking our predictions for next year. I still hold to my 2013 concerns, but I wonder If you were asked to rate confidentiality, integrity and availability in order of importance what your answer would be? First, it may depend on your definition of each. Second, it may depend on what has happened recently to trigger a knee-jerk in your company. Third, it may depend on where you anticipate technology to be heading. This last criteria is one that I view as being of prime importance. Technology moves at a faster pace than our ability to control it. It took us years to notice that real-time systems needed a different control set than that required for batch systems and we are still struggling to deal with the internet and cloud based applications. I recently watched a BBC horizon programme which supported Snowden's revelation by reporting that quantum computing was capable of breaking RSA encryption in-flight. Whilst on the one-hand governments may applaud this, as it will enable them to eves-drop on other governments and criminal enterprises, it also means that their own communications can be dissembled. I have long argued that the next major conflict will be won by the side with the fastest computers, as these devices are at the heart of modern welfare. Even guerrilla style conflicts are open to intercepted communications, which is why the likes of Al Qaida have resorted to person-to-person communication. Slow, but difficult to intercept electronically.

Fred Hoyle, one of the great astronomers (although he was wrong about the 'steady-state' theory of cosmic evolution), wrote a novel about an alien energy cloud which surrounded the earth and sucked-up electronic waves. Within a short while it was necessary to forego electricity and return to more primitive forms of energy generation and communication. So the next big security issue is likely to be the slowing down, or completely stopping, a company, or nation's computing capability. If you review SC Magazine's top ten threats for 2013 almost all of them relate to availability in one form, or another. You cannot commit espionage without access to the secrets, the insider threat requires access to the service, cloud computing is dependent on the internet, DDoS and sabotage remove the service, botnets abuse the service and mobility requires the service.

Most enterprises, whether local, national, or international, are aware of the need to distribute their processing for resilience, but this puts them at the mercy of the interconnections. Remove the network and the individual devices are pretty much useless. As the network is unlikely to be managed by themselves they are reliant on the infrastructure suppliers to provide the necessary resilience. The internet backbone is quite resilient from a routing viewpoint, but rather like a supermarket's logistics, where it's the last fifty yards to the shelf that matters, so it is with the web. The last fifty yards is as important as the previous three thousand miles. I have a UPS to keep my server and internet router alive for about ninety minutes. Sufficient for minor interruptions, but inadequate in the event of a significant disaster. I have a standby configuration elsewhere, but that itself is reliant on the internet, so my biggest security issue is the external infrastructure.

You will notice that I have answered my initial question. To me, availability is my prime security concern for 2014. I suspect that this is true of governments too. What's the use in being able to crack an encrypted message if there is no medium for such traffic? The various governments need to keep the infrastructure alive in order to deploy their huge computing assets. On the other side, the low-tech terrorist organisations need to kill the infrastructure, on which they are less dependent, in order to prevent the deployment of those assets. Everyone else is piggy-in-the-middle trying to conduct their businesses, either legal or illegal, as efficiently and effectively as possible. We are all reliant on others to provide and manage the infrastructure. When John Glenn, the first American to orbit the Earth, was asked what he was thinking about during the trip, he answered 'that every component was supplied by the lowest bidder'. My fear too.

John Mitchell

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of BCS Council, the Audit & Risk Committee 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