Information Security Now – 8

John Mitchell

Getting to grips with information security is like trying to decide whether you are on the inside or outside plane of a moebius band. No matter which way you look at it, no matter which way you turn something eludes you. The jelly wobbles and the blancmange collapses at just the moment you think that you have it finished and therein lies the problem with information security: it is never finished. Information technology expands just like the universe, with dizzying speed. The Hubble red shift has nothing on what has happened with IT since the nineteen fifties. At first momentum was slow. Very little movement in the mainframe environment for a couple of decades and then the rapid expansion of storage technologies, networking and end-user computing. Then with even dizzier speed the reduction in size of components bringing mobile networking, personal digital assistants and radio frequency identification. Implants which are currently in their infancy will become common place, especially if governments get their way. New technology raises new security challenges and by default new control problems to be solved.

As devices became physically smaller physical security became more difficult to enforce. As an example ten thousand mobile devices are simply lost on the London transport system each year. add to this the number stolen in robberies, or left behind at the security screening areas in airports and you have a large potential exposure. So we close this exposure by adding logical security ranging from simple PINs through to biometric scans such as fingerprint recognition. Considering that most mobile telephones provide for internet access to office systems the simple PIN is woefully inadequate. If the telephone is stolen whilst it is on-line, then the thief has access to the associated office systems. Many users do not even use a PIN and have the telephone/PDA configured to automatically log on once the device is switched on. Blackberry users never seem to switch them off anyway. We then consider multi-factor authentication, but as we already know from cash machines, the criminals then simply apply the threat of injury to obtain the access credentials. With PDAs there is some merit in using proximity alarms. If the PDA moves out of range of the proximity monitor it could be programmed to automatically shut down. This would cover the risk of loss as well as theft. Likewise if you wish to protect data from unauthorised access, then splitting a key data between (say) three separate locations will complicate the problem for the hacker as s(he) now has to break into three systems to obtain anything useful.

The careful application of the confidentiality, integrity, availability and compliance (CIAC) framework using risk assessment and management techniques enables even complex technologies to be broken down into their key aspects. How can we keep things secret and accurate? How can we make sure that they get to the people who should have them when they need them? How can we remain legal? I was recently dealing with a government department which wish to release a new internet based tool to enable certain parts of the community to gain access to personal data stored on a government database. Using risk analysis techniques I was able to quickly establish that the developers had done an excellent job in preventing unauthorised access to the data. However, what about unauthorised disclosure by an authorised user? There was nothing the IT people could do to prevent that scenario. It could conceivably be detected after the event if the sensitive data entered the public domain, but by then the damage would be done. A typical outcome of applying risk analysis techniques to data leakage. In this case we have relatively low likelihood, but very high consequence (reputation, breach of trust and conceivably non-compliance with legislation). The politicians have two clear choices: terminate the risk by not deploying the tool, or tolerate the risk and be damned if it crystallises. Tough call, but that's what they get paid for. I get paid for pointing out the risks and the available choices. Mine is the easier of the two jobs.

John is editor of BCS IRMA's award winning *Journal* and Managing Director of LHS Business Control, a corporate governance consultancy that he founded in 1988. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454.