Editorial

John Mitchell

The military are trialling the use of RFID tags to help identify its assets and to reduce the incidents of friendly fire (an oxymoron only slightly worse than 'military intelligence'). For 'assets' read: machinery, vehicles, weapons and wetware (people). You can imagine the scene as an American F22 swoops down on a truck in the desert. 'Confirming identification of truck …. Oh, oh, it's one belonging to the Brits and its got six special forces guys on board and they are all wearing Calvin Klein boxer shorts'. Now think of the problem faced by of one of our chaps dressed in mufti in order to infiltrate a terrorist cell. 'Okay Siddique, scan him with the RDIF reader. Well, well, a nice pair of M&S socks under that well worn robe, please step into this nice little room …….'.

At the moment the military test versions (much more rugged than the civilian equivalent apparently) require 4 AA batteries to power them, so a battery failure reverts you to potential enemy status. Perhaps there is an opening here for a wind-up version as part of the army's BCP? 'Keep cranking trooper. You are the only thing between us and oblivion'. The downside scenarios are endless: a faulty batch of chips, power failure, duplication, substitution, forgery, poor data base administration, interface failure, etc. The whole RFID thing is something that we need to get to grips with quickly. We need to identify the risks and assess the controls. Once again the technology appears to be moving ahead of our ability to control it. as it has done so many times during the forty years that IRMA has been in existence.

One of the amazing things about controlling the technology over the last four decades is that the underlying principles of confidentiality, integrity, availability and compliance have remained unchanged. Sure the technology has moved on, but this has not negated the underlying methodology for assessing the risks. We can control the technology and manage the people. These are not quite the same thing. We manage people by implementing policies, standards and procedures, but until we can implant a chip we are still unable to control them. That is what makes auditing so fascinating. It is not the computer that steals the money, but a person. A computer does not carry out a denial of service attack unless subverted by a person. The abnormal program abend is caused by the programmer, not the program. So people management is really important and that is one reason why I argue that security is a human resource challenge. After all it is HR that conducts the background check. It is HR that sets the employment policies and staff review processes and it is HR that drives the termination process. All in all, it is a pretty solid case for HR driving security. Indeed, perhaps the chief security officer should be part of HR? It is certainly worth opening the debate.

Last month we provided a free full-day technical briefing for our members as a way of celebrating our fortieth anniversary and you can see some of the

photographs from that event elsewhere in this edition, together with a letter from Fred Thomas who was a previous Treasurer of the group. You will also find an interesting paper by John Leach on Threat Based Security Engineering, another from a team at Portsmouth university on development risks, a report from our current chairman Alex Brewer, a down-under column from Bob Ashton and an update on our parent body from Colin Thompson.

Remember, this is the last printed edition of the Journal. Next year we go fully electronic so we need your email address. A move into the electronic age after forty years. Is that progress, or what?

The compliments of the Season to you all from your Management Committee.