Editorial

John Mitchell

They that can give up essential liberty to purchase a little temporary safety deserve neither liberty or safety.
--Benjamin Franklin

Some months ago, Alex Brewer the then Chairman of this group, pointed out that the new British passports contained a wi-fi transponder which had not been widely mentioned in all the ho-hah relating to the proposed bio-metric passports. Indeed, the roll out of this relatively undocumented feature had already commenced and his daughter's passport was so enabled. The Government stated that the encryption used was triple DES and no-one need concern themselves about passport identity theft by someone interrogating the chip. Now the basic rule of encryption is that you assume that the other side will know the process, but hope that they do not know the key that you are using. However, with these passports to key is actually displayed in the printed part of the passport itself. It comprises the passport number, the holder's date of birth and the passport expiry date. All of which, as reported by the Guardian[1] newspaper, are often required at hotel registration desks to get a room. If you couple that information with an RFID scanner (£174 at your favourite electrical store) you can suck out all the biometric information from the chip and create your own perfect clone. I accept that you still need to forge the actual passport, but it probably does not need to be a perfect copy as the immigration authorities will most likely rely on the data in the chip. If fingerprint recognition is used, then you can use the data in the chip to create the matching set on silicone which then fit snugly over your real prints. The Home Office claim that you have to be really close to the chip to interrogate it, but the Guardian researcher was able to do so from a distance of thirty metres which included a couple of walls in the way too.

A few years ago I predicted that with the roll out of RFID chips in the retail sector the criminals of the future would only have to scan you, your car, or your house to decide if you were worth robbing. I was laughed at by the consultants selling the technology on two grounds. First, all chips would be disabled once the product left the store and second the distance thing already mentioned. I did not believe at the time that the first would happen and even if it was so intended it would not be perfect and I had no faith at all in the distance argument as advances in technology would enable that to be solved. My advice is to use disinformation. Obtain a load of RFID chips that identify your clothes as being from ASDA and not Amarni, your watch as a Timex rather than a Rolex and showing your ring as containing zircon and not diamond. Go one stage further and carry with you another chip containing passport information belonging to someone else (preferably someone well

[1] 17th November 2006

known for their martial arts skills) to give the muggers something to think about when they "read you". Here is another prediction, the term "to read you" will enter the English vocabulary in much the same as "to Google" already has, but with far more serious undertones.

As someone once said, if you want to eat an elephant do it one small piece at a time as otherwise you will get acute indigestion. What they don't say is which piece you should eat first? Providing assurance on IT can be like eating an elephant, but at least we have a guide as to where we should start. General controls first, followed by the specifics. As the applications rely on the infrastructure and the infrastructure comprises the hardware, base software and network stuff, then it's pretty obvious that an accurate asset register is the starting point. If they haven't got that, then how can the CIO know that things are well controlled? IT comprises around 34 key processes with all the associated interactions. If we can measure the absolute maturity of each process and its relative importance to the other processes, then we have a further indication as to where we should target our resources. We have great toolkits available to us ranging from CobiT[2] through ISO 27001, ISO 20001, ITIL and ISO 9126 to name but a few. We also have associated qualifications such as CISA[3] and CISM[4] which indicate our professional attainments. Put this heady mix together and we become pretty much invincible in justifying the work that we do and the assurance that we can provide. Co-active auditing as I call it (working with the clients rather than against them) does not mean us lying down with our legs in the air, but it does require a degree of confidence that I often see sadly lacking in many IT auditors. Forget about friendship, it's respect that we crave. To get that you also have to have it for the other side. Mutually assured respect (MAS) is something we need to work on. They need to as well.

In this edition Bruce (Harv) Busta, Kris Portz, Joel Strong & Roger Lewis bring us the results of their research into the most important controls for small businesses. Ryan Purita educates us on computer forensics, while Bob Ashton draws our attention to the worlds of virtual cime. Jean Morgan reports on our financial situation and Mark Smith has provided his usual helpful list of members' benefits which shows the value for money you receive from your membership subscription. Lou Agosta deals with the thorny subject of governing data governance and Davis Clarke our parent body's CEO covers the need for professionalism. Which is where I ended up in my editorial.

The compliments of the season to you all and I hope to see you at our next meeting in the New year.

Don't forget to volunteer for your Management Committee. We are really desperate to persuade someone to help us with membership.

---

[2] Control Objectives for IT from the Information Systems Audit & Control Association
[3] Certified Information Systems Auditor
[4] Certified Information Security Manager