Editorial

John Mitchell

This is the first edition of the Journal to be issued solely in electronic format. Although you have been able to access the Journal on-line for some years now we have persisted in sending out a hard copy version as many of us prefer the ability to browse off-line, away from our desks. Alas, the expense of hard-copy production has now become unsustainable so we will only be publishing future copies as an Adobe PDF file on our web page. From there you can either browse on-line, as you may well be doing now, or download it to your personal device for off-line viewing, or actually printing it on your local printer. The access password will be changed every six months, but you will be informed of this via our regular email communication with you, so it is essential that our administrator has your latest email address (admin@bcs-irma.org).

One of the things that I advise companies on is business continuity planning (BCP) and there is always a spurt of activity after a disaster; viz 9/11, 7/7 and Hemel Hempstead. One of my regular findings is that very few firms seem to have their change programmes linked to their business continuity planning; this assumes that they are managing change in the first instance. Few companies consider BCP when they re-structure and even less when they outsource a process and yet these often have a greater impact on the BCP than a change to a computer system. Business continuity planning is a key component of disaster recovery planning (DRP), in that DRP is the later aspect of BCP. That is, your business continuity has failed and you now need to recover the situation. It's amazing how many auditors do not see the entire continuum, but BCP is about keeping the show on the road while DRP means that you have crashed. Reviewing your BCP and eliminating, so far a is possible, the single points of failure is usually far cheaper and less disruptive than having to invoke the DRP. Also, DRP testing is often very expensive, if you can do it at all. I am much in favour of desk-top walk through tests on a regular basis, as being a reasonable alternative to a proper test. They can be done frequently, with different staff and reflecting different scenarios. Audit can umpire these tests by determining the scenario at the last moment and 'killing off' some of the participants to see how well their deputies can manage without having to make the actual funeral arrangements. It's great fun too!

For good BCP/DRP you need a configuration management database (CMDB). In simplistic terms this is a superior asset register, usually with a relational database so that you can predict the impact of removing, adding or changing one of the assets. The CMDB is useful for establishing the minimum configuration needed to run a particular application and enables you to create what if type scenarios, such as the loss of a file, media, server or router. Very handy for identifying single points of failure without actually pulling the plug. Like all software tools however, it is only as good as its data and this is where the link to change management becomes important.

On a regular basis I receive emails warning me of some dire thing that is being perpetrated only to find out that it is actually a hoax. Invariably these start off with “a friend of mine ………………..”, or more alarmingly “the police have warned …….”. I immediately feed the lead words into my search engine to find the source of the warning and invariably find that the hoax is already well established. It’s a bit like the urban myths of the 1990s, but the hoax hoax (that’s my name for these) can now be spread so much faster. Some are not so harmless in that they persuade their victims to delete system files or to reveal credit card details, but the majority are just time wasters. What does amuse me is how defensive the relayers of these hoaxes become when I point out that they have been duped. I guess that it’s a bit like being on the end of a less than favourable audit report.

The ID card bill progresses through Parliament with the likely cost varying widely depending on who is speaking. On the basis of past government system developments the centralised database, which is key to whole thing, has about as much chance of working as intended as the attempt to pea nuts in Kenya in the middle of the last century. A more misguided solution to a non-problem is hard to imagine.

This edition concentrates on submissions from the antipodes. The major contribution is a paper defining a model to support information security governance from a combined team representing Queensland and Hong Kong universities, while our regular correspondent from that area, Bob Ashton, raises the problems associated with digital rights management. The chairman’s column likens software infrastructure to archaeology and Mark Smith rakes up some great member benefits. The humour page is a great antidote to the SAD syndrome.

I hope to see some more of you at our future meetings. They provide good value CPE for many professional CPD programmes and you get decent food and drink too!