Editorial

I had that sense of déjà vu once again last week when I helped out our sister group the Information Systems Audit & Control Association (ISACA) to man (okay, I know that it is not political correct) their stand at COMPSEC. COMSPEC is a mishmash of a conference dealing with security and audit, with the emphasis on the former. As a result most, no all, of the exhibitors are security companies and here comes the déjà vu bit. Not one of these companies had heard of ISACA, only a few knew about the British Computer Society and none of them knew about us. Same story last year and the year before that back to the dawn of time. So we must be missing an opportunity to recruit these people. As I pointed out to them when I raided their stands for freebies (no-one pillages like a computer auditor) it was essential that they involved us in the development of their products and we also provided them with a fairly captive audience to promote their wares. Lots of polite interest, but I got the feeling that they did not see the relevance of 'audit' to them, unless it related to ISO 9000 or TickIT. Which brings me nicely to a new qualification that may be of interest to you. The Certified Information Security Manager (CISM) qualification has been developed by ISACA to plug a gap in the security qualification arena. There is already CISSP (Certified Information Systems Security Professional) available, but that qualification is aimed squarely at practitioners. The CISM is aimed at security managers and the first examination is scheduled for June 2003. In the run up to the exam and in order to kick start the qualification ISACA is offering a 'grandfather' route to certification. For fuller details go to www.isaca-london.org. The CISM may well help to bridge the gap between us and the security profession on the basis of set a thief to catch a thief!

Now on to other, but related issues. Technology appears to be moving faster than our ability to control it, but that is only a surface appearance. It doesn't matter whether it's a mobile telephone, or a main-frame computer the control basics really haven't changed since the inception of real-time systems in the last century (mid 1980s, but last century sounds *really* ancient). Identify the user, authenticate the user and allocate them appropriate privileges. Monitor usage, keep out the lords of darkness and ensure confidentiality, integrity and availability. Not too much to ask, but these attributes need to be designed in from the start and not band-aided on after implementation. Hence the need for us and the security people to get together at the requirements stage, even before the design takes shape. After all, control should be a requirement of every system, regardless of its infrastructure and audit are secondary users of all systems so our requirement for read only access to everything should also be a requirement. Get these two things into the requirements specification and all the good things should flow from them as part of the system development methodology. Indeed, by concentrating on confidentiality, integrity and availability we cover all the major control aspects. By bringing in ISO 17799 we can provide the security professionals with an international standard to boot. Looking at it from that point of view we should not just be having a relationship with our security friends we should actually be sleeping with them (Chairman of ISSG be warned!). As I spend a lot of my time facilitating security and control workshops I have ceased to be amazed at the lack of understanding of basic control concepts by security people and, more sadly, by the inability of most auditors to define what a control is and how it actually operates.

I had a bit of fun at our most recent one day event on IT Governance in teasing the audience on this latter point, but it is a really important issue. If we auditors cannot

define in understandable business terms what a control is and how it operates how can we expect to get a sensible message over to the gung ho computer people who just want to deliver a workable system in an impossible time scale? At least by hanging our hat on ISO 17799 we can provide them with a sensible framework, but before we go down that road we need to understand the under pinning of ISO 17799. How many of you have even read it, let alone interpreted it and then decided the bits that are relevant to your organisation. ISO 17799 is fairly unique as an international standard in that it lets you leave things out provided that you can make a case for doing so. I cannot understand those organisations that are not adopting it and here I am not promoting accreditation to the standard, but simple adoption of the principles. The fact that it can be tailored to the needs of an organisation gives no reason for non-compliance. In fact I can imagine the situation in the near future when the FSA, or some other regulatory body, has the CEO of a company in the dock as a result of an IT failure. The conversation will go something like this. 'So you knew about ISO 9000, but didn't adopt it. What did you have that was better? Oh, a mishmash of policies, standards and procedures, but were these really better than the international standard?'. If you want to protect your CEO or CIO from such a scenario, then you had better get to grips with ISO 17799.

On a lighter note I understand that Harvey Jones, a previous chairman of ICI and now a company 'doctor', said that 'planning was an unnatural process. It is much better to do something and when you fail it comes as a complete surprise rather than spend six months worrying about it in advance'! So much for ex captains of industry. I don't think that I would have had much success in persuading Mr Jones to plan for his company's future.

So what's in this edition? The main paper is from Fiona McGregor who examines the problems associated with digital images. Andrew Hawker focuses on computer forensics, while Bob Ashton examines the problems of securing wireless telemetry which is increasingly used to control important parts of any country's national infrastructure. Colin Thompson, the Deputy Chief Executive of the BCS provides his usual wealth of information about our parent body.

And finally, a big welcome to John Ivinson the new BCS president. John has been a tireless worker in promoting IT security and audit. He was the force behind the founding of our sister group, the London Chapter of ISACA and I hope that he will have time to come along to one of our events.