IRMA
Information Risk Management & Audit
◆ A specialist Group of the BCS ◆

JOURNAL

volume 13 number 2 autumn 2002 ISSN 0961-9348

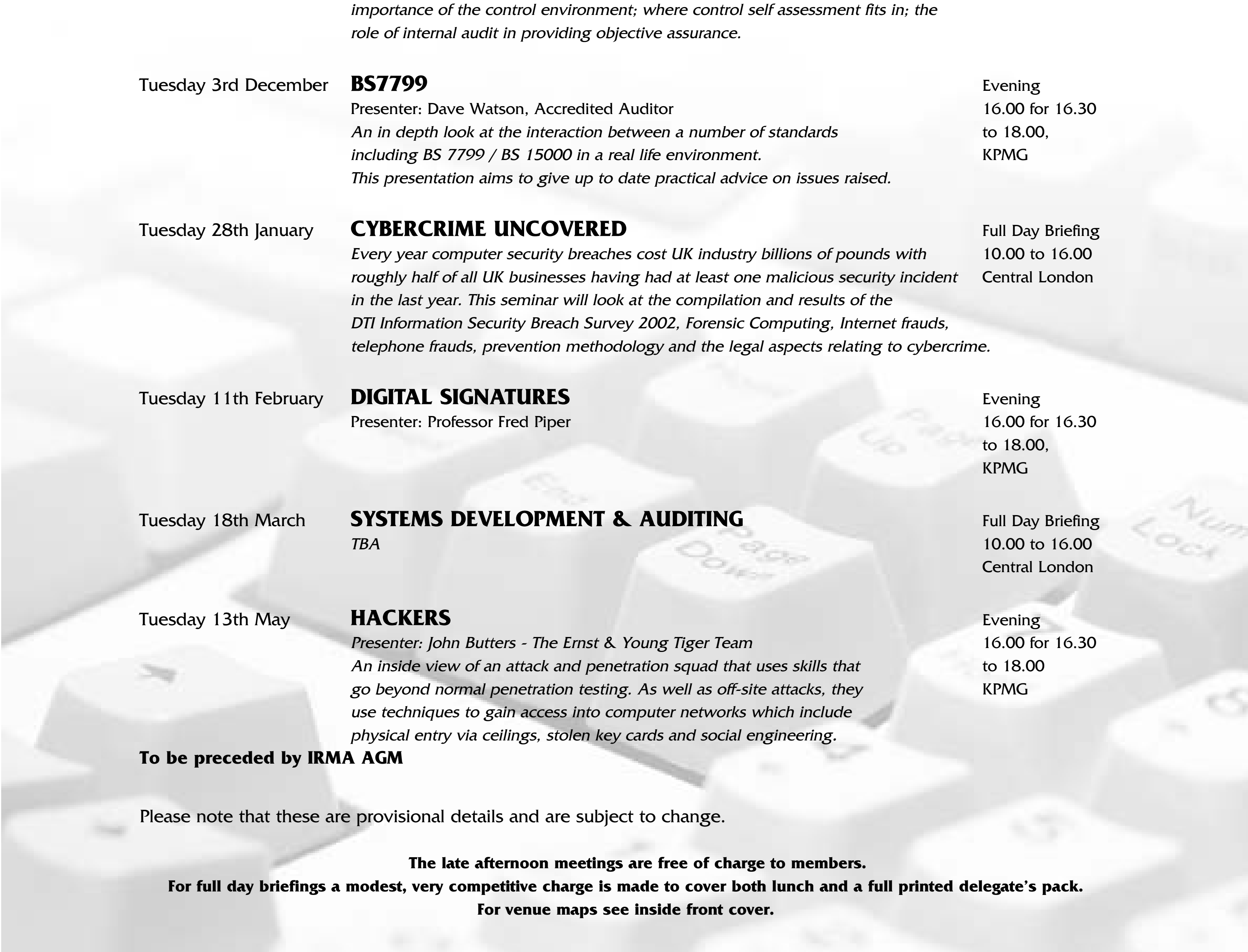
Programme for members' meetings 2002/2003 season

Tuesday 1st October	**DATABASE SECURITY** Presenter: Alex Brewer, Lloyds TSB	Evening 16.00 for 16.30 to 18.00 KPMG
Monday 4th November	**IMPLEMENTING AND AUDITING IT GOVERNANCE** Joint Meeting with IT Faculty *Turnbull upset the apple cart by stating that organisations should consider not only their financial controls, but also their risk management processes, compliance and operation controls. This has put many IT departments on the spot as they now have to assure senior management that they have appropriate processes in place to meet these requirements. One way of achieving this is to implement an appropriate IT governance programme. This seminar examines: the concepts of IT governance; the role of risk management in the process; the importance of the control environment; where control self assessment fits in; the role of internal audit in providing objective assurance.*	Full Day Briefing 10.00 to 16.00 Chartered Accountants' Hall Moorgate Place London EC1
Tuesday 3rd December	**BS7799** Presenter: Dave Watson, Accredited Auditor *An in depth look at the interaction between a number of standards including BS 7799 / BS 15000 in a real life environment.* *This presentation aims to give up to date practical advice on issues raised.*	Evening 16.00 for 16.30 to 18.00, KPMG
Tuesday 28th January	**CYBERCRIME UNCOVERED** *Every year computer security breaches cost UK industry billions of pounds with roughly half of all UK businesses having had at least one malicious security incident in the last year. This seminar will look at the compilation and results of the DTI Information Security Breach Survey 2002, Forensic Computing, Internet frauds, telephone frauds, prevention methodology and the legal aspects relating to cybercrime.*	Full Day Briefing 10.00 to 16.00 Central London
Tuesday 11th February	**DIGITAL SIGNATURES** Presenter: Professor Fred Piper	Evening 16.00 for 16.30 to 18.00, KPMG
Tuesday 18th March	**SYSTEMS DEVELOPMENT & AUDITING** *TBA*	Full Day Briefing 10.00 to 16.00 Central London
Tuesday 13th May	**HACKERS** *Presenter: John Butters - The Ernst & Young Tiger Team* *An inside view of an attack and penetration squad that uses skills that go beyond normal penetration testing. As well as off-site attacks, they use techniques to gain access into computer networks which include physical entry via ceilings, stolen key cards and social engineering.*	Evening 16.00 for 16.30 to 18.00 KPMG

To be preceded by IRMA AGM

Please note that these are provisional details and are subject to change.

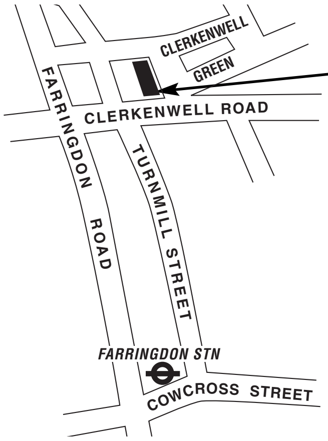
The late afternoon meetings are free of charge to members.
For full day briefings a modest, very competitive charge is made to cover both lunch and a full printed delegate's pack.
For venue maps see inside front cover.



Contents of the Journal

Venue for Full Day Briefings

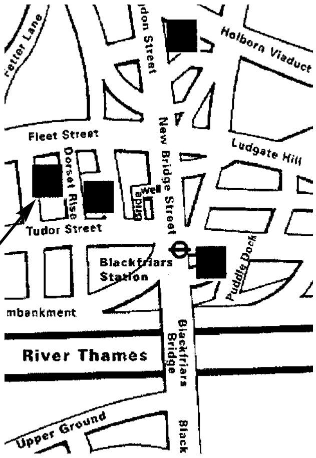
(except 4 November 2002)



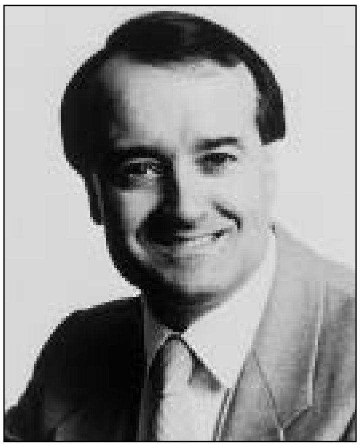
Old Sessions House
Clerkenwell Green
London EC1

KPMG
8 Salisbury Square
London EC4

Venue for Late Afternoon Meetings



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. COMPSEC 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

The views expressed in the Journal are not necessarily shared by IRMA. Articles are published without responsibility on the part of the publishers or authors for loss occasioned in any person acting, or refraining from acting as a result of any view expressed therein.

Editorial Panel

Editor
John Mitchell
LHS Business Control
Tel: 01707 851454
Fax: 01707 851455
Email: john@lhscontrol.com

Academic Editor
David Chadwick
Greenwich University
Tel: 020 8331 8509
Fax: 020 8331 8665
Email: d.r.chadwick@greenwich.ac.uk

Editorial Panel
Andrew Hawker
University of Birmingham
Tel: 0121 414 6530
Email: a.hawker@bham.ac.uk

George Allan
University of Portsmouth
Tel: 02302 846415
Fax: 02392 846402
Email: george.allan@port.ac.uk

BCS Matters
Colin Thompson
British Computer Society
Tel: 01793 417417
Fax: 01793 480270
Email: cthompson@bcs.org.uk

Events Reporter
Rupert Kendrick
Tel/Fax: 01234 782810
Email: RupertKendrick@aol.com

Australian Correspondent
Bob Ashton
Wide Bay Capricorn Building Society Ltd
Tel: +61 7 4159 0649
bob_ashton@excite.com

The ***Journal*** is the official publication of the Information Risk Management & Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

Letters to the editor are welcome as are any other contributions. Please contact the appropriate person on the editorial panel.

Editorial address:
47 Grangewood,
Potters Bar
Herts, EN6 1SL
Email: john@lhscontrol.com

Designed and set by Carliam Artwork,
Potters Bar, Herts
Printed in Great Britain by PostScript,
Tring, Herts.

Editorial continued

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 17799, 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.

John Mitchell

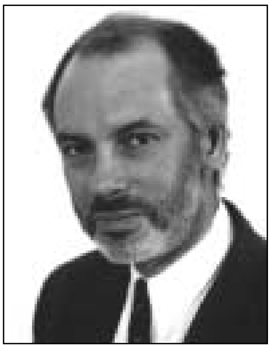
Chairman's Corner

John Bevan

Participation is essential to any vital group. We need more of our members to join the committee and help in running the group. Please don't skip the rest of this piece, because you may well be able to get more benefit out of helping us than the time you put in. After all committee members pay nothing to attend our full day events, make potentially useful contacts in the risk management world, and can add "professional activity" to their cv's.

We are looking for two new committee members to help us grow both our membership and meeting attendance, and thereby eliminate the operating loss we have made in recent years.

The first job is marketing co-ordinator: to find and co-ordinate the many small, and often cheap, ways to promote or advertise the group. For example: if a commercial conference organiser or training firm wants IRMA to advertise an event, we can do so if in return he advertises IRMA to his customers. When promoting IRMA, we obviously want to present as attractive a picture as possible. One way to do this is always to have a programme of meetings arranged for the next twelve months. This is why we need someone to fill the second job, that of programme co-ordinator, to identify attractive meeting topics and delegate to other committee members the job of organising individual meetings.



Also, because I have been on the committee for a long time, I would like to see additional younger members on the committee. There are other jobs, such as organising a particular promotional campagn or meeting, which you may like to do. To find out more, and especially if you feel cautious about volunteering, phone a committee member (see elsewhere in the journal and on the website), discuss the matter, and perhaps come to a committee meeting to see what happens, before making up your mind. If you have your own ideas for what else the group might do, then please get in touch with a committee member. You would all be very welcome!

Imaging Systems - Evidence Compliance

By Fiona McGregor

Introduction

The timing of this paper, as the last paper of the conference[1], is in some ways quite applicable. To me, it seems to follow the natural process within many organisations, with the IT gurus approaching management about some "new, great, wonderful, time-saving, workload-reducing IT toy" they've just read about in the latest PC-World or InfoTech Weekly. Sometimes, in an even scarier fashion, it can be the top executives approaching the IT gurus about the new toys. However, what never seems to change is that finally someone considers whether this new shiny knowledge management tool is going to increase risk to the company when it comes to a litigative action where a discovery process is underway. In terms of document imaging, in many countries governments have gradually caught up with what's going on. They've reacted to this new technology in a reasonably similar fashion, largely with a memory of the way that they approached issues relating to micro-film and photocopying. In the following paper I will look at a few different overseas examples and the tools that have been created by practitioners to cope with admissibility. I'll dwell mainly, however, on admissibility issues here in New Zealand and how these foreign tools can assist in minimising risk.

Fear of the Unknown

It is well known that where technology leads, the judiciary and relevant case law gradually follows. It is to this end that business enthusiasm must be tempered by sound legal advice - the sort of stuff that I, as an archivist and policy worker, can not provide. This is not to say, however, that as an employee of National Archives of New Zealand, I don't have any requirement to know about these issues. Daily my colleagues and I are called on to provide records' management advice to central and local government over what to do with overflowing shelves of records. We therefore need to keep up with the play regarding the effective management of all types of records. From my research, there seems to be fairly common approaches to the vexed issues of admissibility in Canada, the US, Britain, Australia and New Zealand. Issues relating to this topic tend to have centred on

- Proving the technology
- Proving the process

In many ways this reflects past experiences with changes in technology. Sarah Piasecki, a well-known archivist writing on admissibility issues in the American Archivist, agrees:

> *The legal questions being raised [in 1994] about the legal admissibility of electronic records recall previous debates over the introduction of two other technologies: photocopies and microfilm. Both of these technologies were distrusted as evidence until the law was able to establish bases for authenticating them as true reproductions of paper originals. It remains to be seen how the law will handle electronic records. Early evidence indicates that it is seeking to stress the similarity of electronic records to paper and microfilm records and to define conditions for the establishment of dependable systems of electronic record keeping.* [2]

To take up her first point, that "technologies were distrusted ...until the law was able to establish bases for authenticating them", I can cite two cases, to illustrate the point: the first relating to the early nineteenth century, the second more locally, the Equiticorp case, Rowland v. Burton The acceptability of non-print information in courts of law has been an issue in the United States of America since at least 1838. In that year a Delaware lawsuit

> *...established an important precedent for the evidential value of non-conventional records. Noah Burton, a free black, sued James Rowland for non-payment of wages for work on Rowland's farm. Burton claimed that Rowland owed him $25.40 for a period of two to three years and offered a notched stick as a record of his work. Despite the legal disabilities facing free blacks in Delaware at that time, Burton successfully sued Rowland before a justice of the peace. Apparently the use of notched sticks was a fairly common method of record keeping among enterprising but illiterate freedmen.*[3]

A supreme court later upheld the ruling, although not citing this common method, instead noting a common law principle that 'regular entries made in the routine of business at or near the time of a transaction' were admissible as evidence. Another example is the Equiticorp case, where all documents were scanned using a Wang system - and the master copy was provided to the Court. The process was acceptable to the court because of the large amount of paper involved and the fact that the original documents still existed. It is interesting to note that this case could also be seen as an example of the functional breakdown of paper documentation, that the court felt it necessary to discard the concept of distributing paper copies when this proved too onerous. [4] From research I've done, advice seems to be that what is likely to be acceptable, is technology that is:

- reliable
- easy to use
- reasonably established
- easy to access.

Overseas Approaches to Admissibility of Imaged Documents

So what is the legal environment overseas for organisations contemplating imaging systems? Take for example:

The Australian Approach

Greg O'Shea and David Roberts in their article for the Australian archives journal Archives and Manuscripts suggest that federal legislators in Australia are taking up the challenge of electronic documents, this being demonstrated through changes effected by the Evidence Act 1995. The Act specifically

- abolishes the 'best evidence' rule
- provides many options for proving the contents of documents the facilitation of proof of public documents, official and business records, and documents and evidence produced by processes, machines or other devices which make it easier to prove a range of formal matters in relation to documents.'
- relaxes and simplifies the hearsay rule, particularly for business, public and official records.' [5]

The British approach

Mike Steemson, a British records management consultant now active in New Zealand, has also spoken about the British approach to admissibility issues. He cites the Civil Evidence Act 1995,

> "Section 8(1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved by the production of that document, or
>
> whether or not that document is still in existence, by production of a copy of that document or the material part of it, authenticated in such manner as the court may approve" [6]

Note that this legislation explicitly leaves the establishment of authenticity to the Court.

British politicians have been active in this issue with other legislation. The House of Lords Select Committee on Science and Technology recommended, in relation to the Data Protection Bill: [7]

> *That the Government encourage the appropriate legal bodies to draw greater attention to the change to digital processing and to widen public awareness that paper originals are rarely necessary*

To which the UK Government's response was:

> *The Government agrees with this proposal but notes that while paper originals may rarely be necessary, retention of the original digital file, captured from the original paper or other source, is considered highly desirable, if not essential.*

And to the recommendation:

> *That the Government encourage the use of authentication techniques. Members of the legal profession should be made aware of the benefits of these techniques, their value in adding weight to evidence and the possible significance of their omission. [Recommendation 3.20]*

The UK Government's response was:

> *The responsibility of proving the reliability and authenticity of data falls to the body carrying out the capture, processing and modification. Thus an audit trail, either electronic or enshrined in operational procedures, or preferably both, is essential. While any digital image can be considered for presentation as evidence, the court would be well advised to place a greater weight on evidence which can be rigorously demonstrated to have been derived from an authenticated original.*

"Weight of evidence" - this is a key concept to be borne in admissibility issues, which I'll also return to later on in this paper. Too often the authentication or not of documents is seen as a black and white issue, when the better the system and processes demonstrated, the greater the weight given to the evidence admitted. As Mike Steemson said recently: "A judge may allow a document into his court, but does not later have to give its evidence any credibility if he is given reason to believe it to be flawed or at least suspect." [8]

In order to improve the chances of admissibility, the British Standards Institute has, in association with interested parties, developed and published a "Code of Practice for Legal Admissibility of Information Stored on Electronic Document Management Systems" which they hope soon will be accepted at ISO level. They have also followed this up with a workbook that managers can complete and present at hearings when imaged documents are submitted as evidence. [9]

The co-authors of the Code (of which Mike Steemson is one) have identified "five separate areas of control impacting on evidential record-keeping in image storage systems. They set them out as:

- Representation of Information
- Duty of Care
- Business Procedures and Processes
- Enabling Technologies
- Audit Trails

I will go through this code of practice later in this paper, within the section emphasising the importance of good record keeping, as a means to admissibility.

Canada

Research that I have undertaken shows that the Canadian Information and Image Management Society (CIIMS) standards committee has developed "the Microfilm and Electronic Images as Documentary Evidence Standard" to provide a structure and guidance for organisations to "establish and operate a credible image management program". This standard has been approved by the Standards Council of Canada and has gained further government support with Revenue Canada, the government tax-collecting body, accepting electronic copies of financial records if they have been created and maintained in accordance with its recommendations. [10]

The New Zealand Experience

Jeanette Watson, a senior associate of the law firm Rudd Watts & Stone, described the New Zealand approach at an electronic records management conference last year:

> *"The rules in this area are quite complex, but in general the court will not admit computer-generated information, or will not rely on it, unless it can be satisfied that (a) the source of the information is authentic; (b) the information has been accurately and completely recorded; and (c) the information has been completely and accurately reproduced"* [11]

In May 1994 the New Zealand Law Commission published a preliminary paper relating to the use of documentary evidence.[12] It detailed that the "common law" rule of admissibility currently requires that 'before a document is received in evidence its authenticity must be shown by evidence extrinsic to the document itself'. The Law Commission suggested that in this case the common law was unsatisfactory, and that the requirement for extrinsic evidence should be removed - the document to be 'self-authenticating'.

More recently, the Law Commission has indicated[13] that a new Evidence Code will go some way to facilitating the use of electronic data as evidence - the keyword being 'relevance' of documentation whether that be electronic or paper. The concept of 'original document' is to be removed, as it can be irrelevant in the electronic context. Having called for submissions the Commission is now in the process of preparing a final report, which is due in December this year. Together with the report will be an Evidence Bill, both of which are to be tabled in Parliament. The Government will then need to decide whether to promote this Bill which will replace the current (much-amended) Evidence Act, promulgated initially in 1908. In the meantime, however, legal advice should be sought when the imaging of business records is contemplated, as your legal advisors will have the most up to date information on what courts will accept and the weighting they might give to documentation.

The Law Commission, has also previously suggested that WORM (Write Once Read Many) systems are favoured by the legal profession. This is particularly the case

> "where a business' records or systems are kept in a way that the records can easily be altered. This would probably affect the weight that is given to the document. For example, if the court is told that a document has been retrieved from a disk on which you write once, then the weight given to that document may be greater than evidence produced from a disk that is capable of being amended.[14]

So where does this leave the New Zealand records manager? To return to the first of the "twin tennets of admissibility" I mentioned earlier - "proving the technology", imaging components (both software and hardware) are more likely to be admissible if they conform to industry standards. If the technology is proven to be "complex or unusual", then expert evidence may be required to prove the "reliability of the machine and outputted documents".

In relation to the second of the "twin tennets of admissibility" I mentioned earlier - "proving the process" a well-crafted information plan and allied record keeping system including audit trails will assist when admissibility of imaged records is required.

Unfortunately, the results of a recent survey by my group at National Archives of government record keeping practices has been the source of some disappointment for my colleagues and myself. After a healthy 72% return rate, the collated responses showed that

- 48% of government agencies had no records management policies at all (although the core public sector had the highest levels of policy documentation)
- databases and networked PCs are heavily prevalent in agencies (71% and 82% respectively)
- electronic document management systems are present in less than half of all agencies (22% of agencies are considering their adoption)

It seems that some improvement in records management is required here - and I fear that central government reflects what is happening in other sectors!!! Perhaps government agencies could learn much from overseas approaches. I'd like now to quote Sarah Piasecki again regarding the American experience, as I feel her article is equally applicable here. In this passage from American Archivist, she discusses the recommendations of a 'white paper' issued by the U.S. Justice Department relating to the rules of evidence as applied to electronic records. Apparently the document asserts that while the same rules of evidence apply to both paper and electronic records, 'judicial thinking should be tempered by knowledge of the ease with which electronic records can be manipulated and altered'. In Piasecki's view:

> inadequate documentation or inability to explain these controls in laymen's terms can have dire consequences either in getting such evidence admitted or in the weight it is accorded in terms of probative value.

The British Code of Practice I mentioned earlier agrees:

> "It does not follow that documents held on systems that do not conform to all the essential processes and procedures in this Code are not legally acceptable. However it is likely that it will be more difficult to prove their integrity in a court of law".

Graham Smith, of the Information Technology Group, Great Britain, has described the British situation in this way:

> "potential users of document imaging systems have often expressed concern as to whether the images will be admissible as evidence in court if they destroy the original documents. The simple answer to this question under English law is in most cases 'yes'. However, mere admissibility is not enough. Admissibility means only that the court will look at the product of the imaging system. The user must also consider how useful those images will be in court compared with the original document. There are respects in which images... are potentially and inescapably less useful than the original document. Successful use of imaging systems requires proper assessment and management of these risks (especially as to selection of documents for imaging and destruction), based on an understanding of these issues. [15]

The British Code of Practice that I mentioned earlier has been developed to address these points and I feel it will be a useful tool here in New Zealand also. To run through the five sections in detail:

Representation of Information

This section proposes that information held within a document management system needs to be "classified" according to its life-cycle. Accordingly, classification can be used to determine storage options and procedures. Issues to be address include rules relating to:

- creation
- retention period
- access
- revisions
- destruction

The format of the documents being managed must be addressed, as the format will obviously also determine storage options and procedures.

Duty of Care

The standard states at the beginning of this section

"It is essential that an organisation is aware of the value of information that it stores and execute its responsibility to that information" under this principle.

This section therefore describes the need

- to establish a "chain of accountability", assigning responsibility for activities "involving electronic document management at all levels"
- to monitor flows of information throughout the organisation
- to identify legislative impacts and the controls of regulatory bodies pertinent to their organisation
- to have agreed and documented levels of security for managing its information (with reference to another BSI-published code of practice on information security management).

Business Procedures and Processes

The requirement to create a "comprehensive user manual" describing "every process, electronic and physical, affecting the operation of the electronic archive". This documentation should be fully followed so that it is possible to demonstrate to lawyers or auditors that the document system conformed to the Code at appropriate times. This user manual could also form part of the information requirements for ISO 9000 certification.

The Code details the types of data a user manual should collect, including:

- Document types
- Preparation of documents prior to scanning
- Scanning processes
- Batch control
- Compression techniques
- Quality control
- Indexing
- System maintenance
- Backup and recovery
- Use of bureau services
- Remote transmission of data files

There is a note that an annual audit should also be carried out, with the review signed off by the person responsible for the operation.

Enabling Technologies

This section describes computer technologies and how they can be utilised and controlled, including;

- the use of a systems description manual
- documenting access levels
- use of audit logs
- image processing - post scanning improvement needs to be documented
- controls for storage of component parts of compound documents
- compression techniques

Audit Trails

A record needs to be kept of every "significant" activity, and must be automatically generated by the technology. This record must be readily accessible to people not familiar with the system, with instructions on access identified in the user manual. The type of information to be generated includes:

- accurate date and time of initiation of process
- amendments to index files
- name of operator
- workstation reference

Canada

I mentioned earlier the Canadian "Microfilm and Electronic Images Documentary Evidence" standard. Key concepts in this standard, which could equally be applicable here, refer to:

- creation of an Image Management Program (IMP)
- the need to collect evidence to prove sources of data and information
- data was collected close to date of imaging
- data regularly supplied
- data is not subject to legal privilege
- entries made in regular course of business
- entries conform to standard industry practice
- business confidence in data - use of data relatively recently
- software reliability
- documentation of all procedures including automatic recording of date and time of scanning
- security measures are in place to ensure the integrity of the system.

AS4390 - the Australian Records Management Standard

The Australian Records Management Standard comes highly recommended as a world-first and because of its sound suggestions for reliable recordkeeping practices. Created by our nearest neighbour, this standard has been recognised as "state of the art" technical reports at ISO level. It has also been noted that adherence to this standard may cover the "quality records" requirements of ISO 9000 certification. Keith Parrott, Director of the Documentation Standards Project, Australian Archives, commented in 1996:

> "Part of the ISO 9000 requirements is to produce quality records. The AS4390 records management standards sets down best practice for the creation of quality records. This standard is also very important for information management activities." [16]

The standard encompasses these parts:

- General (contains definitions and describes briefly the other parts of the standard)
- Responsibilities (identify regulatory environment and who is responsible to comply with the standard, design of policies such as those relating to implementation)
- Strategies (need for strategies to ensure adequate evidence of business activity is being retained, capturing and converting of existing data, monitoring and compliance processes)
- Control (such as classification and registration, indexing and tracking)
- Appraisal and disposal (including functional analysis, design and application of disposal authorities)
- Storage (discussion of records storage concepts, physical features of records, preservation issues) [17]

Adherence to this document will surely provide an advantage in presenting imaged documents for admissibility. National Archives fully supports the work of the Standards New Zealand Records Management Committee in its furtherance of aims to develop this document as a joint standard.

Our mandate for involvement in current record keeping practices comes from the Archives Act and the Local Government Act. We therefore involve ourselves in learning about the new "knowledge industry" and "information economy" and spreading the information so that we're not the last port of call. It is in this way that we can achieve better archival outcomes in the records management continuum.

Summary

In summary, I hope I've made the following points:

- Difficulty of legislation to keep up with advances in technology
- Demonstrating the common approaches of the judiciary
- Authenticating the technology worked correctly
- Auditing the record keeping process
- Describing some of the tools created to ensure that admissibility is achieved

My Conclusion?

Through using appropriate technology with appropriate controls you'll minimise risk to your organisation.

Foot Notes

1 This paper was first presented at the Electronic Document Management conference, SkyCity, Auckland, June 1998.

2 Sarah Piasecki "Legal Admissibility of Electronic Records as Evidence and Implications for Records Management" American Archivist Winter 1995 (Volume 58) pp54-64

3 Meyer H Fishbein, "The Evidential Value of Nontextual Records: An Early Precedent" American Archivist, Vol. 45, No. 2 Spring 1982, pp 189-190.

4 "Admissibility of information stored in electronic format" research prepared for Wellington City Council by Phillips Fox, lawyers [unpublished]

5 Greg O'Shea and David Roberts, "Living in a Digital World: Recognising the Electronic and Post-Custodial Realities", Archives and Manuscripts, Vol 24, No 2, (1996), pp 286-311.

6 Steemson, Michael, Caldeson Consultancy,1998: "How to Make the Law Love Your Image", paper presented to the 4th International Records Management Congress in Edinburgh, Scotland, 1998: http://www.caldeson.com/admit.html

7 House of Lords [UK]: "Select Committee on Science and Technology Eighth Report" http://www.parliament.the-stationery-office.co.uk/pa/ld199798/ldselect/ldsctech/121/12101.htm

8 Steemson, 1998 British Standards Institute (1996) Code of Practice for Legal Admissibility of Information Stored on Electronic Document Management Systems, DISC PD0008, BSI: London, UK

9 MetaConcepts: "Legal Admissibility of Electronic Images in the Financial Services Industry" Steemson, 1998

10 Law Commission, Preliminary Paper No.22. Evidence Law: Documentary Evidence and Judicial Notice : A Discussion Paper, Wellington, 1994.

11 Author's conversation with Judge Margaret Lee, Commissioner, New Zealand Law Commission, July 1998.

12 Michael Hoyle "Standard Setting, Monitoring and Compliance in Records Management and Archives Management" Records Management & Technology Conference, AIC, Plimmer Towers, February 1997

13 Internet site: http://www.twobirds.com/

14 Parrot, Keith, quoted in GATEway, Consultancy Services Unit, Australia; August 1996.

15 Standards Australia, 1996:

16 AS4390 - Records Management; Standards Australia, New South Wales, Australia.

17 This page can be found at http://www.archives.govt.nz/archivesnz/staff/papers/imaging_systems.html (c) Archives New Zealand. 2002-2003

Fiona McGregor worked at National Archives from 1991-98 as an archivist in the Christchurch and Wellington offices, and as an archives analyst in the Statutory Regulatory Group. She has also held other positions at the *Department of Internal Affairs,* N Z Forest Service, *Ministry of Forestry* and *Statistics New Zealand* in policy, database management, help desk and training roles. She holds a Bachelor of Resource Studies (Lincoln University) and an Advanced Certificate of Business Computing (Wellington Polytechnic).

Wastewater Control Systems: Australian Case Illustrates Threat and Risks

The following recently appeared on the US Government's National Infrastructure Protection Center site - **www.nipc.gov**

Wastewater utilities need to evaluate a wide range of elements from hazardous chemical storage to the physical and electronic security of treatment and monitoring processes to guard against criminal/terrorist actions. As computer networks and digital monitoring and control technologies continue to play an increasing role in the water industry, risks posed by breaches in electronic security become more widespread.

In the spring of 2000, Maroochy Shire, a community on Australia's Sunshine Coast, began having a series of problems with its wastewater system. In one particularly damaging incident in March 2000, a failure at a pumping station caused up to one million liters (264,000 gallons) of raw sewage to flow onto the grounds of a local tourist resort and eventually into a storm sewer. The problems were traced to disruptions in the community's new computerized sewage control system. Suspicion fell upon a former employee of the company that had installed the control system. On 23 April 2000, police intercepted Vitek Boden, less than an hour after another control system malfunction. A search of his vehicle found a two-way radio and antennae, a remote telemetry system, and a laptop computer.

Authorities subsequently charged Boden with perpetrating at least seven sabotage attempts against the community's sewer system, alleging he used his computer and telemetry units to manipulate the computerized control system via remote radio transmissions. Prosecutors stated that the deliberate sewage overflows cost the community approximately $95,000 in repairs, monitoring, clean-ups, and extra security resulting in significant damage to the environment and to the quality of life of local residents.

In October 2001, an Australian jury found Boden guilty of 30 charges in connection with the incidents. Sentenced to one year in prison for willfully causing serious environmental harm and two years for computer hacking and theft of equipment needed to effect access, he was also ordered to pay approximately $7,000 in compensation to the local council whose systems had been penetrated.

This incident has broad application to the wastewater industry and its related sectors.

- Although not directly connected to the Internet or other public networks, all remote telemetry and control systems are at risk from both external and insider attackers experienced in enterprise networks including intrusion, manipulation, malicious code, and denial of service. Malicious actors are able to purchase, steal, build, or otherwise obtain specialized electronic equipment needed to access even obscure and proprietary electronic systems.
- The threat posed by insiders should also include former employees and contractors who may have motive to exploit their insider access and/or knowledge of control systems and specialized equipment.
- Control and telemetry systems should be monitored for possible trends that may evolve into malicious activity.

Implementers need to consider access control and authentication issues for infrastructure control systems carefully, including access to default or system accounts or any other account that may have been active during system development and testing. Passwords should be changed regularly and all access should be reviewed if system irregularities are suspected. Depending on the architecture, various technologies such as call-back connections to known telephone numbers or filtering of incoming connections may help mitigate risks of unauthorized persons accessing control systems.

According to the U.S. Environmental Protection Agency, the United States' wastewater infrastructure includes approximately 16,000 publicly owned wastewater treatment plants and 100,000 major pumping stations. The securing of electronic systems used to control and monitor these facilities will be a significant task. However, the possible consequences of sabotage to our wastewater infrastructures such as: the public health impacts including immediate and long term illnesses, loss of life in worst case scenarios, contamination of drinking water, significant environmental damage, destruction of wildlife, closing of recreational areas, disruption of fishing and other commercial ventures, and deterioration of quality of life, are significant and should be considered.

Membership Musings

Celeste Rush - IRMA Membership Secretary

I would like to first welcome those of you who have recently joined IRMA. Although I had the opportunity to introduce myself at the first meeting of the 2002/2003 season, many of you may not be aware of what my role as Membership Secretary is. Quite simply, I am here to help in all matters relating to you, the member, and would like to hear from you if you have any comments, criticisms (surely not!), and/or suggestions on ways we as a committee can further enhance your membership value.

As I mulled over what I would write for this auspicious occasion, being my debut article for the Journal, the reoccurring theme that crossed my mind was how all matters relating to security risks and countermeasures in the end came down to one factor above all - people.

Enormous amounts of money and time may be spent on security products, anti-virus software, firewalls, IDS, audits and so on. But no matter what measures are put in place, one person alone could render the entire effort useless or ineffective. One example of this may be the result of an employee falling victim to an extremely effective ploy known as social engineering. Kevin Mitnick, the convicted hacker noted for his considerable social engineering skills, talked about this when testifying to the US Congress in 2000.

"I was so successful in that line of attack that I rarely had to resort to a technical attack. Companies can spend millions of dollars toward technological protections and that's wasted if somebody can basically call someone on the telephone and either convince them to do something on the computer that lowers the computer's defenses [sic] or reveals the information they were seeking." (Schneier, pp 267)

Another way could be from sabotage within by a disgruntled employee. An example of this is the 1996 case of Timothy Lloyd, a network manager at Omega Engineering, who wrote a logic bomb program (a type of Trojan horse) into a large software application to be activated if he was ever removed from the company payroll. The cost of the damage to his former employers amounted to more than $12 million. (Schneier, 2000) (Therein lies a lesson for your Security Policy.)

Other ploys involving malicious insiders include data diddling, espionage, fraud and embezzlement.

However, the non-malicious insider is just as capable of causing severe damage through ignorance and carelessness. There are many reported cases (and many not reported!) where the 'trusted' employee has inadvertently sabotaged a computer system or caused a serious security breach. Only one person needs to open a virus-infected email or attachment to cause havoc and loss. By not following proper procedures, huge amounts of data can be lost or corrupted in a wink of an eye.

How people perceive risks is an important factor. Many studies show that people have trouble evaluating risks even with adequate information and will continually estimate incorrectly in either direction. Lack of information most certainly exacerbates the problem. Unfortunately, much of the risk game is down to probabilities. Flip a coin enough times and, although you may expect an equal outcome of getting heads or tails, you may actually get an outcome of 60-40 in favour of heads. Is this because the coin was not fair?

This is equally true in cryptography where the math is largely based on probability. The renowned cryptographer and security consultant, Bruce Schneier, illustrates as follows:

"Public-key cryptography uses numbers that are probably prime; there is a one in a billion chance that the number is not really prime. One-way hash functions are only probably unique; there is a 1 in 2^{80} chance that two random documents will have the same SHA hash value. The AES encryption algorithm has 2^{128} different keys; there is a 1 in 2^{128} chance that an attacker will correctly guess the key on the first try." (Schneier, pp 258)

Nothing in this world is an absolute certainty.

Indeed, the challenge to break the RC5-64 bit encryption algorithm has been met this summer after four years of effort. The group called Distributed.net used 331,252 volunteers to process millions of hours of work over 1,757 days and on 58,747,597,657 work units. A total of 15,769,938,165,961,326,592 keys were tested when a simple PIII-450 in Tokyo returned the winning key, 0x63DE7DC154F4D039, producing the plaintext output:

'The unknown message is: some things are better left unread.'
(Distributed.net, 2002)

The project has shown what relatively few individuals can accomplish, given the power of the Internet and distributed computing.

More seriously however, the Advanced Encryption Standard (AES) appears to have now been broken through theoretical cryptanalysis.

Cryptographers Nicholas Courtois and Josef Pieprzyk published a paper outlining a new attack on Rijndael (AES) and Serpent (an AES finalist along with Twofish). The paper claims to break the entire algorithm with only one or two known plaintexts. Interestingly, Serpent, the most conservative of the two and the one considered the safest choice, was broken first.

The new attack technique is called XSL, based on XL, which was presented at Eurocrypt 2000. Schneier describes the attack in his recent newsletter, Crypto-Gram.

"Basically, the attack works by trying to express the entire algorithm as multivariate quadratic polynomials, and then using an innovative technique to treat the terms of those polynomials as individual variables. This gives you a system of linear equations in a quadratically large number of variables, which you have to solve. There are a bunch of minimization [sic] techniques, and several other clever tricks you can use to make the solution easier. (This is a gross oversimplification of the paper; read it for more detail.)" (Schneier, 2002)

Got that?

Whether the attacks actually work is not yet clear but recent developments have given cryptographers second thoughts about the future of the current AES.

Throughout the world, there are people willing to go to great lengths to challenge any 'so-called' secure system. Perhaps it is only human nature after all.

Please remember us to your colleagues whom perhaps would like to join us and also share the benefits of membership. This 2002/2003 season should offer topics of interest to all.

References

Distributed.net (2002), 'RC5-64 Has Been Solved', (c) Distributed.net 1997-2002, available at Internet < http://www.distributed.net/pressroom/news-20020926.html >

Schneier, Bruce (2000), Secrets and Lies: digital security in a networked world, Wiley Computer Publishing, USA

Schneier, Bruce (2002), 'Crypto-Gram Newsletter September 15, 2002',
(c) Counterpane Internet Security, Inc., available at Internet
< http://www.counterpane.com/crypto-gram-0209.html >

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should either be on double spaced, single-sided A4 paper, e-mail, or in Microsoft Word, Word-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality monochrome photograph, or electronic image.

Submission Deadlines

Spring Edition	7th February	Autumn Edition	7th August
Summer Edition	7th June	Winter Edition	7th November

The Web Page

Elementary, my dear Pentium

Andrew Hawker
University of Birmingham

"His eyes were sharp and piercing, save during those intervals of torpor to which I have alluded; and his thin, hawk-like nose gave his whole expression an air of alertness and decision. His chin, too, had the prominence and squareness which mark the man of determination". This should not have left villains with any doubts. Not much was going to escape the scrutiny and tenacity of the great Sherlock Holmes.

When tracking down today's computer villains, it is essential to be able to deploy the right kind of forensic tools, as well as a more traditional mix of guile and cunning. For one thing, the quantities of information to be sifted and analysed can be enormous, and at the end of the investigation there must be enough watertight evidence to present in court, (this, however, being a problem which hardly ever seems to crop up for famous fictional detectives).

Computer forensics is a comparatively young science, but there are now plenty of web sites which deal with everything from the more theoretical principles to the supply of relevant products and services. The following is intended to give a flavour of what is available out there. As usual, the mention of particular commercial sites is not intended to suggest any kind of endorsement.

Firstly, there are the information providers. If you have a fairly clear idea of what you are looking for, then the site at the US Department of Justice (**www.usdoj.gov/criminal**) contains a large range of materials, and has a good search facility. There are also some useful articles in the reference library at the IIA (**www.theiia.org**), although this is rather less geared to investigative work.

Then there are the consultancies. Most of these are US-based, which rather limits their use to browsing for more general advice and perhaps their case studies. Among those based more locally in the UK are companies such as Datasec (**www.datasec.co.uk**) based in Hertfordshire, Computer Forensics Ltd in Rugby (**www.cyber-forensics.ltd.uk**), and Computer Investigations (**www.computer-investigations.com**).

Many of the US consultancies have quite extensive web sites. Although these often imply that they are offering a wide range of advice and references, the materials in question often proves to be rather short and fluffy. Their advice may also be based very specifically on the procedures which are required under US Law. Examples here are Computer Forensics Inc at **www.forensics.com**, and Vogon at **www.vogon-computer-evidence.com**.

Finally, there are the suppliers of forensic tools, both hardware and software. Most auditors are familiar with IDEA, which is now marketed at **www.audimation.com**. This has evolved a long way from its early life as a general audit extraction tool, and may well be the initial choice as an investigative tool by those who already familiar with it. Another contender is ENCASE, from Guidance Software, at **www.guidancesoftware.com**. This offers similar features for digging and sifting data, but with perhaps more of an emphasis on overcoming obstacles where it is suspected that information is being withheld or concealed. Some software tools also claim to deal with the particular problems of hunting for evidence in image files, as in cases involving pornography. An example of one such product can be found at the New Technologies Inc site, at **www.forensics-intl.com**.

Another long-standing and familiar product is DIBS, which provides a means of taking quick and accurate copies directly from computer disk drives. Sales of the DIBS workstation are now managed by DIBS USA Inc, at **www.dibsusa.com**. (Readers interested in learning about how this product came to leave the UK can find out from the Computer Investigations site, mentioned earlier).

A recurring feature in many of the sites is a certain amount of bragging about the more spectacular cases which the staff or the products have helped to solve. From these glowing accounts, you might be led to feel that forensic work is both exciting and inspirational. Given the tedium involved in much of it, I have my doubts. As for the literary style of the narratives, it has to be said that Dr Watson would probably have put things rather differently. Holmes, nevertheless, might just have found it all intriguing enough to have a broadband connection installed in Baker Street.

From the Cash Box

Jan Lubbe - IRMA Treasurer

The Committee completed the budget for 2002/03. Our aim is to minimise the annual loss while continuing to perform our planned activities. For 2002/03 we have budgeted for a small loss of £1,080, which compares well with the loss of more than £6,000 last year. This is a healthy financial position, especially if you take into account that we have a cash balance in excess of £30,000. The Committee also tracks the financial position on a quarterly basis and we are on budget after the first quarter.

Apart from controlling costs appropriately, we also need to make sure that we get the income we expect. Although our membership fees is only part of our income, I am glad to report that to date 191 members paid membership fees (50 up on the same time last year). This is a positive sign indeed! The committee wishes to thank everyone that paid already and would like to urge all our other members to make sure all membership fees are paid.

BCS IRMA SPECIALIST GROUP ADVERTISING RATES (Nov 2002)

Reach the top professionals in the field of EDP Audit, Control and Security by advertising in the BCS IRMA SG Journal. Our advertising policy allows advertising for any security and control related products, service or jobs.

For more information, contact John Mitchell on 01707 851454, fax 01707 851455 email john@lhscontrol.com.

There are three ways of advertising with the BCS IRMA Specialist Group:

The Journal is the Group's award winning quarterly magazine with a very defined target audience of 350 information systems audit, risk management and security professionals.

Display Advertisements (Monochrome Only) Rates:

- Inside Front Cover £400
- Inside Back Cover £400
- Full Page £350 (£375 for right facing page)
- Half page £200 (£225 for right facing page)
- Quarter Page £125 (£150 for right facing page)
- Layout & artwork charged @ £30 per hour

Inserts can be included with the Journal for varying advertising purposes, for example: job vacancies, new products, software.

Insertion Rates:

For inserts weighing less than 60grams a flat fee of £300 will be charged. Weight in excess of this will incur additional charges:

• 60-100grams:	14p per insert
• 101-150g:	25p per insert
• 151-300g:	60p per insert
• 301-400g	85p per insert
• 401-500	105p per insert

Thus for an insert weighing 250g it would cost the standard £300 plus weight supplement of £210 (350 x 60pence) totalling £510.

Discounts:

Orders for Insert distribution in four or more consecutive editions of the Journal, if accompanied by advance payment, will attract a 25% discount on quoted prices.

Direct mailing

We can undertake direct mailing to our members on your behalf at any time outside our normal distribution timetable as a 'special mailing'. Items for distribution MUST be received at the office at least 5 WORKING DAYS before the distribution is required. Prices are based upon an access charge to our members plus a handling charge.
Access Charge £350. Please note photocopies will be charged at 21p per A4 side.

Personalised letters:

We can provide a service to personalise letters sent to our members on your behalf. This service can only be provided for standard A4 letters, (i.e. we cannot personalise calendars, pens etc.). The headed stationery that you wish us to use must be received at the Office at least ten working days before the distribution is required. Please confirm quantities with our advertising manager before dispatch. If you require this service please add £315 to the Direct mailing rates quoted above.
Discounts: Orders for six or more direct mailings will attract a discount of 25% on the quoted rates if accompanied by advance payment

Contacts

Administration
Janet Cardell-Williams,
49 Grangewood, Potters Bar, Hertfordshire EN6 1SL
Email: janet@carliam.demon.co.uk
Website : www.bcs-irma.org

BCS IRMA Specialist Group Advertising Manager
Eva Nash Tel: 01707 852384 & 07813 348220
E-mail : eva@nash141.freeserve.co.uk

BCS MATTERS!

Colin Thompson, BCS Deputy Chief Executive, reviews some of the current BCS news items. Further information on these or any other BCS related issues may be found on the BCS Web site (http://www.bcs.org)

Information is also available from Customer Services at The British Computer Society, 1 Sanford Street, Swindon, SN11HJ (e-mail to marketing@hq.bcs.org.uk)

In considering the news items for coverage in this edition of the Journal I find myself somewhat spoiled for choice, such is the level of activity across the Society at the present time. Items competing for attention include proposed changes to the governance arrangements, a possible new membership structure and some ambitious plans from the new Chief Executive to reshape the BCS agenda and the organisation. The Annual Report also deserves a mention as does the progress in a number of product and service areas. I shall endeavour to do justice to all of these items in the space available.

Governance

Since it achieved its royal charter in 1984, the Society has been governed by a Council of 46 members, made up partly of elected representatives of the members and partly of representatives of the Branch and Specialist Group communities. Like many other professional bodies and charities, the BCS is now examining whether this is the best arrangement for the governance of a modern business. This work is being led by Alastair Macdonald, the immediate past president, and options currently under consideration include the creation of a two tier structure comprising a representative Council with advisory powers and a much smaller board of trustees with the main executive responsibility. These proposals are scheduled for further discussion at the Council meeting at the end of November and, if agreed, they will be put to an extraordinary meeting of members early in the new year before submission to the Privy council for the necessary changes to the Charter.

Membership Structure

The possibility of a submission to the Privy Council provides the opportunity to review the BCS membership structure - which has also seen very little change since 1984. Despite some changes to the process for admitting new members over the past few years, there is some evidence that potential members are still confused by the structures and requirements and that they are frustrated by the lengthy application process.

The current review was set up on the basis of four main objectives:

- ◆ Simplify the membership structure and make it more understandable to the IS community.
- ◆ Broaden the base of BCS membership and make it more inclusive
- ◆ Maintain the standards of our core qualification and links to the Engineering Council
- ◆ Take account of - but not necessarily follow - what other institutions are doing in the market-place

In the context of the final bullet point, the most significant changes are those planned by the IEE which will effectively make the MIEE qualification available at point of graduation for those with a 'relevant' academic qualification.

Proposals to be considered by Council on November 24 include the possibility of separating professional membership from Chartered status to allow for a very substantial simplification of the requirements for membership and the associated processing. Under this option the detailed scrutiny and assessment would take place at the point of upgrade to Chartered status, rather than at the point of entry to professional membership.

The 2002 Annual Report

The BCS Annual report published in September shows another excellent year for the Society with continued growth in almost all areas. Total income for the year, at £12.6 millions, is more than 40% up on the previous year with professional products, including ECDL and ISEB showing the strongest growth.

ECDL

Much of the income growth over the past few years has been driven by the success of our major professional product lines, of which the European Computer Driving Licence is clearly the most successful.

Colin Thompson
BCS Deputy Chief Executive

Those of us who have watched the growth of ECDL over the past 6 years should by now be used to its spectacular performance. But I confess that I was surprised to discover recently that the number of UK participants had reached 500,000. That represents a very significant achievement for the BCS but, more importantly, it is a major contribution to the computer literacy programme for the UK.

Alongside the increase in the participant numbers, the ECDL product range is also increasing. The new advanced level qualification was launched earlier this year and, in October, the BCS announced a new certification scheme for ECDL trainers. The new Certified Training Professional Programme (CTP) is intended to raise standards of ECDL training and to promote best practice by validating trainer competence.

The BCS is also extending the reach of the ECDL products into new market areas through schemes such as its schools programmes. This aims to promote the ECDL core skills qualification for 10 to 16 years olds. More than 140 schools have already adopted ECDL as their basic computing skills qualification.

In addition to this activity, the BCS also has a substantial interest in the company ICDL Asia Pacific that holds the licence for the ECDL qualification for much of East Asia, including China.

ISEB

The IS Examinations Board has been the other major BCS success story of the past few years. More than 15,000 people sat ISEB certificates last year and we now accredit over 80 training providers. The portfolio of ISEB qualifications also continues to grow, with the latest addition being the launch in July of a new higher level exam for Software Testing Practitioners. ISEB already has a foundation certificate in software testing and this new qualification is aimed at experienced testing practitioners, enabling the demonstration of in-depth knowledge of testing topics and the ability to perform testing activities in practice.

The New Chief Executive

David Clarke has now been in the Chief Executive's seat for 6 months and he has spent a significant part of that time, with his senior management team and the Honorary Officers, reviewing current performance and making plans for future direction. The results of all that activity have been distilled into a presentation which David and I have been making to various BCS audiences over the past few weeks. The full presentation runs to 90 odd slides and takes us around 2 hours to deliver - so I will not attempt even a shortened version. But it is, I think, worth including the content of two of the slides. Firstly one that sets out the mission of the BCS as we see it:

Change the perception of Information & Communication Technology (ICT) and the individuals who work in it, from one where government , business and the public in general feel that ICT has not delivered on its promises, to one where the ICT profession is considered THE model of high quality professional people delivering important ,consistent, high quality products and services at the time and price they are needed.

And secondly part of the final summary that sets out some of the key actions required:

1. Represent the industry, not less than 5% of it
2. Make "professionalism" count in the market place.
3. Become much more pro-active
4. Develop professionalism in our own business
5. Develop our strategy for Knowledge Based services
6. Make sure our product development programmes continue to provide the funding we need

All this represents an ambitious programme for the next few years and part of the presentation is devoted to a description of the resources and the organisation that will be required at BCS HQ to drive it. That organisation reflects a much sharper focus on key areas such as business planning, press and public relations, support for volunteer activities, overseas development and web content. Twenty three new staff positions have been approved to support the proposed programme and we have completed the recruitment to some of the key positions, including the Head of Business Development, Overseas Development Director and Web Content Manager.

It is, I think, safe to predict that David's leadership will bring an increased level of activity, visibility and excitement to the Society.

Recent Press Releases

A scan through the press releases over the past few months shows up a number of significant external issues - including the recent revisions to the specification for the BS7799 Part 2 Code of Practice for Information Security Management Systems. Willie List, chair of the BCS Security Expert Panel welcomed those changes on the basis that they "introduce a Plan-Do-Check-Act (PDCA) model as the vehicle for creating and maintaining an effective Information Security Management System (ISMS). This will ensure that ISMS is harmonised with other management systems in an organisation."

The press release also records that "The BCS believes the revision has greatly clarified the role of the statement of applicability in relation to the risk identification and treatment process; this makes the relationship to ISO/CIECBS17799 much clearer and explains how to apply the principles established by the Organisation for Economic Co-operation and Development (OECD) to an ISMS".

Security issues also figured in a statement released in September following the news from the new Security Industry Authority (SIA), that a statutory regulatory framework affecting the information and communications industries is unlikely in the near future. The press release quotes David Clarke as saying that.:

"The BCS expressed concerns to the Government on behalf of our membership and others that the provision of information security services appears to fall outside the jurisdiction of the new regulatory body. However, we have subsequently been informed that the SIA does not intend to create an additional regulatory framework for the information or communications industries in the near future."

"The BCS intends to monitor this position and work with the industry and the SIA to ensure that any regulations that may be created in the future are appropriate for the info sec industry's requirements and address its professional status."

"British ICT systems and databases are under increasing attack from fraudsters and hackers, costing the economy billions of pounds annually. This has resulted in a growing demand from both public and private sectors for professional and trustworthy ICT security consultancy that is qualified. This is why the BCS has in place an assessment for security consultants as part of its professional advice register."

And Finally..........

News of the BCS Connect service. All the main elements of the current development stage are now in place and operational. Over 7000 members have registered for the service, which provides them with access to a range of member-only services and benefits together with the facility to update their membership records. The new system also provides some important support facilities for Branches and Specialist Groups - including the ability to update contact details of their members held on the BCS central database - and one of the priorities for the BCS Connect team is now to ensure that we exploit the new facilities to the full across all areas of the Society. We are in the process of recruiting a new BCS Connect Business Change Manager and one of the key tasks for that individual will be to make early contact with all Specialist Groups. In the meantime, Nick Webb, the Specialist Group Support Manager (nwebb@hq.bcs.org.uk) can provide further details.

HUMOUR PAGES

One Liners

1. One tequila, two tequila, three tequila, floor.
2. Atheism is a non-prophet organization.
3. If man evolved from monkeys and apes, why do we still have monkeys and apes?
4. The main reason Santa is so jolly is because he knows where all the bad girls live.
5. I went to a bookstore and asked the saleswoman, “Where’s the self-help section?” She said if she told me, it would defeat the purpose.
6. Could it be that all those trick-or-treaters wearing sheets aren’t going as ghosts but as mattresses?
7. If a man is standing in the middle of the forest speaking and there is no woman around to hear him...is he still wrong?
8. If someone with multiple personalities threatens to kill himself, is it considered a hostage situation?
9. Is there another word for synonym?
10. Isn’t it a bit unnerving that doctors call what they do practice?”
11. Where do forest rangers go to “get away from it all?”
12. What do you do when you see an endangered animal eating an endangered plant?
13. Would a fly without wings be called a walk?
14. If a turtle doesn’t have a shell, is he homeless or naked?
15. Why don’t sheep shrink when it rains?
16. Can vegetarians eat animal crackers?
17. If the police arrest a mime, do they tell him he has the right to remain silent?
18. Why do they put Braille on the drive-through bank machines?
19. How do they get the deer to cross at that road sign?
20. Is it true that cannibals don’t eat clowns because they taste funny?
21. What was the best thing before sliced bread?
22. One nice thing about egotists: they don’t talk about other people.
23. Do infants enjoy infancy as much as adults enjoy adultery?
24. How is it possible to have a civil war?
25. If one synchronized swimmer drowns, do the rest drown too?
26. If you ate pasta and antipasta, would you still be hungry?
27. If you try to fail, and succeed, which have you done?
28. Whose cruel idea was it for the word “Lisp” to have an “S” in it?
29. Why are haemorrhoids called “haemorrhoids” instead of “assteroids”?
30. Why is it called tourist season if we can’t shoot at them?
31. Why is the alphabet in that order? Is it because of that song?
32. If the “black box” flight recorder is never damaged during a plane crash, why isn’t the whole damn airplane made out of that stuff?
33. Why is there an expiration date on sour cream?
34. If you spin an oriental man in a circle three times, does he become disoriented?

Subject: Institutional Phone messages

This is the transcript of the new answering service recently installed at the Mental Health Institute.

Hello and welcome to the Mental Health Hotline.

If you are *obsessive-compulsive:* Press 1 repeatedly.

If you are *co-dependent:* Ask someone to press 2 for you.

If you have *multiple personalities:* Press 3, 4, 5 and 6.

If you are *paranoid:* We know who you are and what you want. Stay on the line so we can trace your call.

If you are *delusional:* Press 7 and your call will be transferred to the mother ship.

If you are *schizophrenic:* Listen carefully and a small voice will tell you which number to press.

If you are *manic-depressant*: It doesn’t matter what number you press & press & press and finally bash; no-one will answer.

If you are *dyslexic:* Press 96969696996969696969696969669696.

If you have a *nervous disorder:* Please fidget with the hash key until a representative comes on the line.

If you have *amnesia:* Press 8 and state your name, address, phone number, date of birth, social security number, and your mother’s maiden name If you can remember which number is 8

If you have *short-term memory loss:* Press 9.
If you have *short-term memory loss:* Press 9.
If you have *short-term memory loss:* Press 9.
If you have *short-term memory loss:* Press 9.

If you have low *self-esteem:* Please hang up. All our operators are too busy to talk to you.

Real Questions About Australia

Here are some of the classic questions that were actually asked of the Sydney Olympic Committee via their Web site, and the Aussie answers that go with them.

Q: Does it ever get windy in Australia? I have never seen it rain on TV, so how do the plants grow? (UK)
A: Upwards, out of the ground, like the person who asked this question, who themselves will need watering if their IQ drops any lower.

Q: Will I be able to see kangaroos in the street? (USA)
A: Depends on how much beer you’ve consumed ...

Q: Which direction should I drive - Perth to Darwin or Darwin to Perth - to avoid driving with the sun in my eyes? (Germany)
A: Excellent question, considering that the Olympics are being held in Sydney.

Q: I want to walk from Perth to Sydney - can I follow the railroad tracks? (Sweden)
A: Sure, it’s only three thousand miles, so you’ll need to have started about a year ago to get there in time for this October ...

Q: Is it safe to run around in the bushes in Australia? (Sweden)
A: And accomplish what?

Q: It is imperative that I find the names and addresses of places to contact for a stuffed porpoise. (Italy)
A: I’m not touching this one ...

Q: My client wants to take a steel pooper-scooper into Australia. Will you let her in? (South Africa)
A: Why? We do have toilet paper here...

Q: Can I bring cutlery into Australia? (UK)
A: Why bother? Use your fingers like the rest of us...

Q: Do you have perfume in Australia? (France)
A: No. Everybody stinks.

Q: Do tents exist in Australia? (Germany)
A: Yes, but only in sporting supply stores, peoples’ garages, and most national parks...

Q: Can I wear high heels in Australia? (UK)
A: This HAS to have been asked by a blonde...

Q: Can you tell me the regions in Tasmania where the female population is smaller than the male population? (Italy)

HUMOUR PAGES

A: Yes. Gay nightclubs.

Q: Do you celebrate Christmas in Australia? (France)
A: Yes. At Christmas.

Q: Can I drive to the Great Barrier Reef? (Germany)
A: Sure, if your vehicle is amphibious.

Q: Are there killer bees in Australia? (Germany)
A: Not yet, but we'll see what we can do when you get here.

Q: Can you give me some information about hippo racing in Australia? (USA)
A: What's this guy smoking, and where do I get some?

Q: Are there supermarkets in Sydney and is milk available all year round? (Germany)
A: Another blonde?

Q: Please send a list of all doctors in Australia who can dispense rattlesnake serum. (USA)
A: I love this one...there are no rattlesnakes in Australia.

Q: Which direction is North in Australia? (USA)
A: Face North and you should be about right.

Q: Can you send me the Vienna Boys' Choir schedule? (USA)
A: Americans have long had considerable trouble distinguishing between Austria and Australia.

Q: Are there places in Australia where you can make love outdoors? (Italy)
A: Yes. Outdoors.

Q: Will I be able to speek English most places I go? (USA)
A: Yes, but you'll have to learn it first.

Golf Story

Shortly after the Pope visited Nation of Israel, Ehud Barak, the leader of Israel, sent a message to the College of Cardinals. The proposal was for a friendly game of golf to be played between the two leaders or their representatives to show the friendship and ecumenical spirit shared by the Catholic and Jewish faiths. The Pope met with his College of Cardinals to discuss the proposal. "Your Holiness," said one of the Cardinals, "Mr. Barak wants to challenge you to a game of golf to show that you are old and unable to compete I am afraid that this would tarnish our image to the world." The Pope thought about this and as he had never held a golf club in his life asked, "Don't we have a Cardinal to represent me?" "None that plays golf very well," a Cardinal replied. "But," he added, "there is a man named Jack Nicklaus, an American golfer who is a devout Catholic. We can offer to make him a Cardinal, then ask him to play Mr. Barak as your personal representative. In addition to showing our spirit of co-operation, we'll also win the match." Everyone agreed it was a great idea. The call was made. Of course, Nicklaus was honoured and agreed to play as a representative of the Pope. The day after the match, Nicklaus reported to the Vatican to inform the Pope of the result. "I have some good news and some bad news, Your Holiness," said the golfer. "Tell me the good news, Cardinal Nicklaus," said the Pope. "Well, Your Holiness, I don't like to brag, but even though I've played some pretty terrific rounds of golf in my life, this was the best I have ever played, by far. I must have been inspired from above. My drives were long and true, my irons were accurate and purposeful, and my putting was perfect. With all due respect, my play was truly miraculous." "How can there be bad news?" the Pope asked. Nicklaus sighed, "I lost to Rabbi Tiger Woods by three strokes."

Le Computer / La Computer

A language instructor was explaining to her class that French nouns, unlike their English counterparts, are grammatically designated as masculine or feminine. For example, a palace is male, "le palais", but a pyramid is female, "la pyramide". Confused, the students asked which gender pronoun to assign to a computer. Since she did not know, the teacher divided the class into two groups, women in one group and men in the other, and told them to decide if it was Le Computer or La Computer.

The group of women concluded that that computers should be referred to in the masculine gender because:

1. In order to get their attention, you have to turn them on.
2. They have a lot of data but are still clueless.
3. They are supposed to help solve your problems, but half the time they ARE the problem.
4. As soon as you commit to one, you realize that, if you had waited a little longer, you might have been able to get a better model.

The men on the other hand decided that computers were definitely feminine:

1. No one but their creator understands the internal logic.
2. The native language they use to communicate with other computers is incomprehensible to everyone else. 3. Even your smallest mistakes are stored in the long-term memory for later retrieval.
4. As soon as you make a commitment to one, you find yourself spending half your salary on accessories for it.

Some classics....

1. I'm not into working out. My philosophy: No pain, no pain.
2. Ever wonder if illiterate people get the full effect of alphabet soup?
3. I always wanted to be somebody, but I should have been more specific.
4. Have you ever noticed? Anybody going slower than you is an idiot, and anyone going faster than you is a maniac.
5. You have to stay in shape. My grandmother started walking five miles a day when she was 60. She is 97 today and we don't know where she is.
6. The statistics on sanity are that one out of every four Americans is suffering from some form of mental illness. Think of your three best friends. If they are okay, then it's you.

IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	John Bevan	Audit & Computer Security Services	01992 582439 john_bevan@ntlworld.com
DEPUTY CHAIRMAN	Pete Biss	EMX Co Ltd	01279 858300 pete_biss@hotmail.com
SECRETARY	Siobhan Tracey	BFG plc	01494 442883 siobhan.tracey@booker.co.uk
TREASURER	Jan Lubbe	KPMG	020 7774 8303 Jan.Lubbe@gs.com
MEMBERSHIP SECRETARY	Celeste Rush		020 8858 7384 RushLSE97@aol.com
JOURNAL EDITOR	John Mitchell	LHS Business Control	01707 851454 john@lhscontrol.com
WEBMASTER	Allan Boardman	Goldman Sachs	07881 930814 webmaster@bcs-irma.org
SECURITY PANEL LIAISON	John Mitchell	LHS Business Control	01707 851454 john@lhscontrol.com
MEMBER SERVICES BOARD LIAISON	Celeste Rush		020 8858 7384 RushLSE97@aol.com
EVENTS	Siobhan Tracey	BFG plc	01494 442883 siobhan.tracey@booker.co.uk
	Alex Brewer	Lloyds TSB	020 7418 3544 alex_brewer@bigfoot.com
	Rosemary Mulley	NabarroNathanson	0118 950 5640 r.mulley@nabarro.com
ACADEMIC RELATIONS	David Chadwick	Greenwich University	020 8331 8509 d.r.chadwick@greenwich.ac.uk
LOCAL GOVERNMENT LIAISON	Peter Murray		01992 582105 cass@peterm.demon.co.uk

Membership Enquiries to:

Janet Cardell-Williams
49 Grangewood, Potters Bar, Herts EN6 1SL
t: 01707 852384
f: 01707 646275
e: members.irma@bcs.org.uk
www.bcs-irma.org