Programme for members' meetings 2003/2004 season

Tuesday 21st October	**WIRELESS NETWORKING UPDATE** Alex Brewer	Late Afternoon
Tuesday 25th November	**E-MAIL MANAGEMENT AND SECURITY** Vogon International	Full Day
Tuesday 2nd December	**PDA's AND MOBILE COMPUTING RISKS** Peter Wood	Late Afternoon

2004

Tuesday 28th January	**COMPUTER AUDIT BASICS, PART I**	Late Afternoon
Tuesday 7th February	**NETWORK MANAGEMENT**	Full Day
Tuesday 16th March	**OUTSOURCING**	Full Day
Tuesday 11th May	**SERVER FARMS**	Late Afternoon

AGM precedes the meeting

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 back cover.

Contents of the Journal

Editorial

With this edition of the Journal you should also have received your renewal advice. There are five types of renewal: corporate main, corporate subsidiary, individual, student and courtesy. The corporate main member pays a subscription of £75 which includes up to four other people from the same organisation. Corporate subsidiary members receive notification that they do not need to take any action, although I highly recommend that they check that their main member is taking responsibility for payment. With transfers of staff and re-organisations it is easy to assume that action is being taken when it isn't! Individual renewals are of two types: BCS members and non-BCS members. The former pay just £15 while the non-members fork out £25. Full-time students receive a special low rate of just £10 to encourage them to take an interest in information systems risk management. Whatever your membership level, please take a moment to renew your subscription. Not only does this entitle you to several editions of this Journal each year, but a scan of the list of either free, or heavily discounted events on the front cover should make you realise what a bargain this is. Subscriptions for other professional organisations often exceed one hundred pounds for a similar, or even lower level of benefits.

There is so much going on along the IT front these days that it becomes increasingly difficult to keep up to date. The dynamics of the technical, social, legal and business environments mean that there are now many fingers in the standardisation and qualifications pie. ISO 17799 requires accredited auditors, but what qualification(s) should they have? The BCS, in conjunction with the Information Systems Audit and Control Association, is currently discussing the matter with one of the main ISO 17799 accreditation bodies. Starting from the presumption that the main role of audit is to provide assurance to senior management we then descend to the playing field of exactly what this assurance is and how should it be obtained? To my way of thinking there are two ways of approaching these questions.

First, what exactly is assurance? According to various dictionaries 'assurance' is a guarantee, so immediately you see why the phrase 'reasonable assurance' tends to be used. We give a reasonable, but not absolute guarantee that things are as management assert them to be. We cannot give absolute assurance without checking every transaction and 'absolute' becomes a nonsense word when we give any assurance over system development. So we settle for reasonable assurance. But what is reasonable? On what do we base the guarantee that we offer? This is where accepted audit practice and standards enter the equation. The audit profession is now well established and has a number of qualifications that indicate a degree of professionalism. CISA and QiCA are both basically saying that the holder has been found to meet a minimum level of competence. Compare this with the IT industry where the majority of participants have nothing that guarantees their professional competence. Before anyone tackles me with the 'I have a degree in computer science' argument let me make it quite clear that this is a measure of educational and not professional attainment. The BCS has only 39,000 members out of an estimated 650,000 people involved in the mainstream UK IT industry.

Now let us examine the thorny issue of standards. The cynicism attached to these never ceases to amaze me. I recently addressed an audience of IT directors on the subject of IT governance. There was almost universal derision from the audience regarding the use of anything like ISO 9000, ISO 9126 or ISO 17799. Some even boasted of their manipulation of ISO 9000 .... and these people were attending to find out about IT governance! When I challenged them on what other basis they should be measured against there was a singular lack of suggestions. So we are in a really strong position. We know that our main role is to provide assurance that IT is supporting the enterprise in a well controlled manner, we are professionally qualified (or should be) and we judge them against internationally recognised criteria. Throw in a bit of risk management and it's game, set and match to us.

Editorial continued

So what in this edition will enhance your knowledge even further? A survey of UK IT managers' views on security policies for starters, followed by an update from Australia on a recent survey there on computer crime and a sad story about stupidity. Colin Thompson provides his usual informative guide on what's happening at the BCS. As a result of the AGM you are now represented by a newly constituted Committee and a number of them have taken the opportunity to introduce themselves in this edition.

I hope that you have a good break and look forward to seeing you at our meetings in the Autumn.

One of the benefits of being an IRMA member is that we sometimes negotiate discounts for key security and audit events. These discounts pay for your membership many times over, such as the £200 discount we have obtained for our members attendng COMPSEC 2003. See elsewhere in this edition for details.

John Mitchell

Chairman's Corner

John Bevan

That was a close call! After my "No volunteers will mean no more IRMA" letter to all members, Jean Morgan offered to stand as Treasurer, and four or five members offered to join the committee. All were duly elected at the AGM - you can read more about them and their responsibilities elsewhere in this and later issues of the Journal. I am delighted that IRMA has survived the crisis and was very pleased to see most of the new faces at our first committee meeting held after the AGM on May 13th. It was a real pleasure to be there - it covered much ground quickly: reaching consensus on important issues, allocating some major responsibilities, accepting appropriate disciplines, and setting a few imminent deadlines (subsequently met).

We are again trying out the idea of a chairman and deputy chairman. The constitution does not define the role of deputy chairman, and needs to be updated if the approach is found to work well. The idea is that the deputy chairman is a member of the committee who assists the chairman, taking on some of his duties by mutual agreement, and learning about the chairman's job, with the intention of standing for the job of chairman in the

normal way at some future date and in accordance with the constitution. It is an approach that works well in other voluntary organisations or groups, providing a clear succession path and visible assurance that a suitable candidate has been identified to be chairman next. Alex Brewer is now deputy chairman.
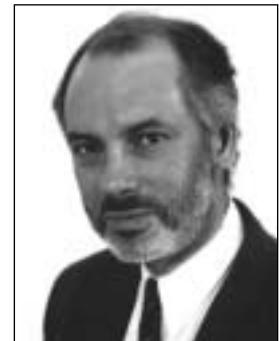
During the crisis described above I wondered if we should blame it in part on a general decline in the number of those in specialised computer audit or information risk management jobs. Or perhaps there are now more "generalists" doing this work alongside other audit or risk management tasks, as someone from a recruitment agency recently suggested to me at Infosec this year. It is difficult for me to assess the extent to which either might be true, but perhaps IRMA's activities need to be changed somehow (how?) to reflect a changed employment market place. I'd be pleased to hear your views on this.

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

Information Security Policy Management

A survey of senior IT managers

Dr Sharm Manwani and Caroline Fraser

Background

In 2001, The British Computer Society (BCS) and Henley Management College (HMC) created a partnership to enhance Business IT management practices. One element of this collaboration has been to undertake joint research projects, leading to the set-up of the BCS Henley Research Panel.

The aim of the survey was to explore opinions amongst a section of Senior IS Managers/Directors within large organisations on a topical issues such as Information Security and promote debate on the subject.

Objective

The specific objectives of this survey were to review the importance of IS Security Management within organisations by assessing:

■ The perception of threats to IS Security

■ The policies and procedures in place to reduce these threats

■ The priority placed upon IS Security by Boards of Directors

■ The role of the BCS regarding Information Security

The following summarises the main findings and key points of the survey.

Conclusions

The survey has highlighted that Information Security is given varying status within organisations and that many Boards are perceived as not taking an active interest in this issue.

IT directors have varying degrees of confidence in the effectiveness of the organisation's Information Security policy. Although most companies have security policies in place many were highlighted as not having full contingency plans for different events that may damage or compromise their systems.

Lower priority was given to promoting a security culture, undertaking education and training, and working fully to established industry standards.

The BCS is seen as having a clear role in the area of Information Security and in particular to actively promote standards and raise awareness of the issues with Company boards and wider IT management.

Those organisations with more proactive Boards address the potential risks for Information Security more comprehensively than those Boards that take a more reactive or little interest in the issue of IS. The results indicate that Information Security should be given a high profile with the Board.

The biggest concerns of IT director respondents related to confidentiality and internal fraud. Hence, it is not necessarily a question of spending significantly more money on technology. Appropriate investments should be made in expertise and training to foster a greater awareness of the potential risks and encourage a security culture.

MAIN FINDINGS

● Information Security is given widely varying status within organisations. Policy is generally the remit of the Head of IT, in three quarters of companies. Responsibility for the execution of the policy is more likely to be a priority for different IT functions within companies, a section of them at a middle manager level.

● Most organisations have some plans in place for serious unavailability threats that might compromise their communications and computer systems. However, the survey highlighted that just less than half of organisations have formalised procedures for a threat such as a bomb or fire demolishing their offices and only a third a formal plan of what they would do in the event of a virus bypassing their security software.

● Breaches in confidentiality (39%) followed by lapses in data integrity (28%) were considered to be more of high risk to corporate data than availability threats through service failures (20%).

● Internal fraud was felt to be the more serious threat to the security of information systems, rated as high or medium by 72% of respondents.

● Over 90% of companies have Information Security policies, operational backups, and security systems in place to avoid or reduce the threats. People investments were less prevalent, with less than 50% listing separation of duties, training, and recruitment of security professionals.

● Of those companies who outsource services, only 60% conducted formal checks of the security policies of their suppliers.

● On standards, 83% fully comply with the Data Protection Act. 50% fully or partly comply with BS7799 Pt 2 or ISO/IEC17799.

● Overall confidence in the efficacy of their organisation's policy on Information Security varied. There was high confidence in the technology aspects with about half the respondents very confident. Medium confidence was shown in business applications, with a quarter of respondents very confident on this. There was relatively low confidence in user issues and an integrated approach with less than one in ten very confident on these aspects of their policy.

- Boards demonstrate a varying level of interest in the issue of Information Security. This coincides with a lack of regular direct feedback to Boards on Security issues. Only a third of respondents felt their Boards took a proactive interest in the issue of Information Security. This was generally because of a wider recognition of the risks associated with any weaknesses or breaches in this area. For more reactive or disinterested Boards, Security was more likely to be seen as an operational issue and the potential risks unappreciated or felt to be less critical to their business.

- The BCS is seen as having a clear role in the area of Information Security and in particular to actively promote standards and raise awareness of the issues with Company boards and wider IT management.

SURVEY RESULTS

Responsibilities

1. The majority of respondents (80%) were IT Directors or Heads of Information Systems and the remainder were either IT Managers or IT Consultants. 28% of respondents saw Information Security as a main responsibility of their job. For the remainder, with the exception of one respondent with no involvement, it was a secondary function.

2. Whilst three quarters of respondents saw Information Security Policy a responsibility of senior IT managers, the actual execution of the policy was a role of various levels of managers within the organisation. The Head of IT, IT Manager, the Operations Manager or the Security Officer reporting to IT were the principal individuals mentioned. This is likely to be a reflection of the status this issue is given within different types of organisations.

Who is responsible for the Information Security policy and execution in your organisation?
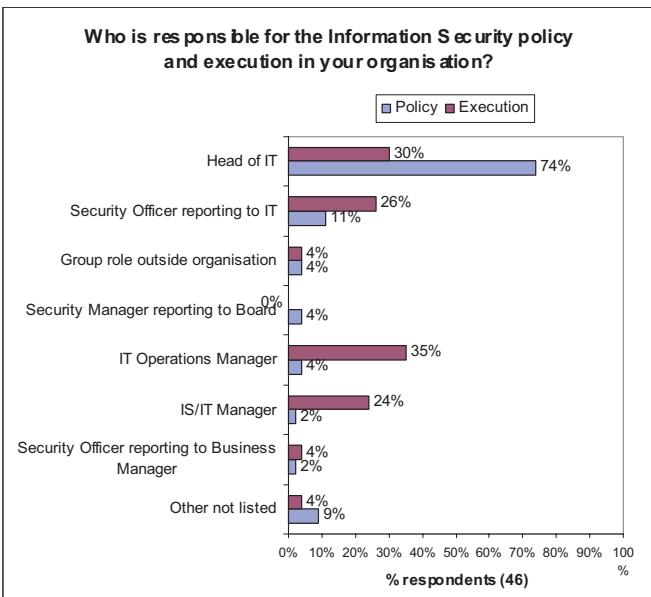
Threats

3. With a view to assessing the degree to which organisations address potential threats to their Information Security, respondents were asked whether they had procedures in place to minimize the business impact of four hypothetical threats.

Over a quarter of organisations had no stated plan for a bomb threat or a breach of access through disclosed passwords.

Just under half of companies had a formalised procedure for what may be a more likely risk, such as their communications destroyed by a bomb or fire. Only a third thought their organisation had a formal procedure in place should their systems be seriously affected by a virus attack.

What plans or procedures are in place to minimise the business impact of the types of event?
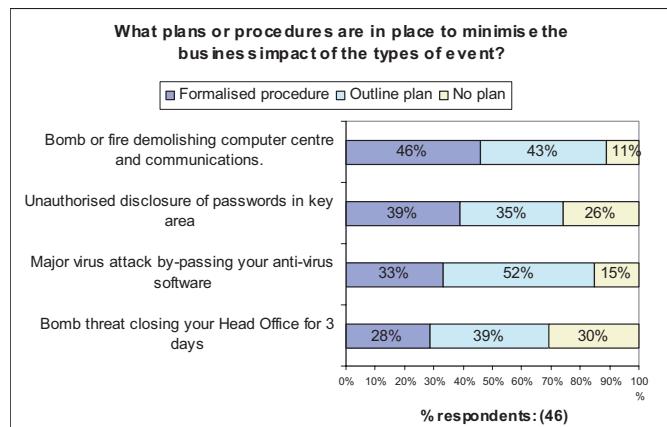
4. Breaches of confidentiality were seen as the greatest potential risk to corporate data rather than availability problems.

What do you consider to be the main potential risks to your corporate data?
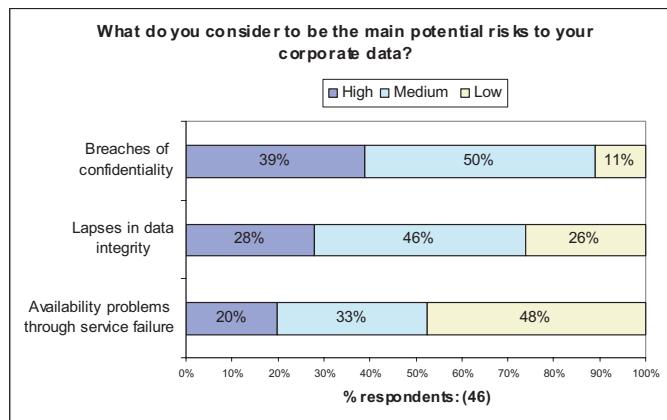
5. Whilst companies may not always have full plans to minimise the threats to their systems, respondents generally demonstrated a confidence in the security of their systems and few saw the list of potential risks as high risk. There was potentially greater risk of problems being generated internally by internal fraud or abuse or errors in the system rather than by external agents.

What do you consider to be the main potential threats to the security of the information system?
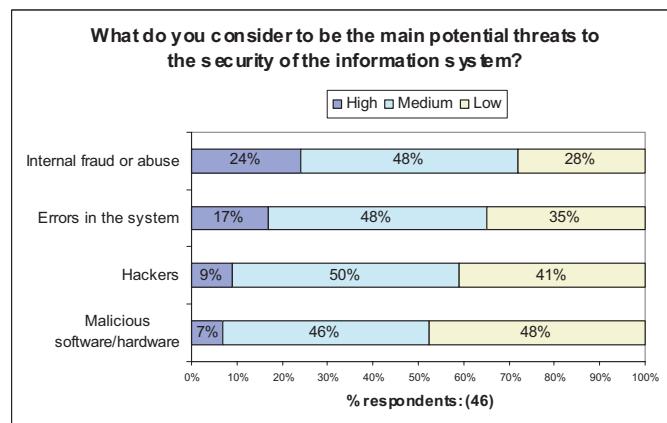
Policies & Procedures

6. Most companies have policies and systems in place to avoid or reduce the threats to Information Security. This ranges from virtually all organisations implementing a Security Policy and adopting software and hardware security measures. Most store back up data off site and two thirds run alternative or back up processes and Security audits. Most companies also restrict staff use personal use of e-mail and downloading from the Internet, a common source of viruses infiltrating systems.

Whilst half of respondents think that a security culture is fostered within their company, less priority is given to people investments such as the recruitment of IS Security professionals (26%) or organising IS Security training (41%) to support that ethos.

How does you organisation avoid or reduce threats?

Storing back up data off site	96%
Implementing Security policy/ISMS	91%
Software/hardware security measures	91%
Company regs. on use of E Mail/ Internet downloading	89%
Running alternative/back up processes	70%
Implementing Information Security audit	67%
Fostering a security culture	57%
Separating duties to avoid conflicts of interest	46%
Organising IS Security training and awareness	41%
Recruiting IS Security professionals	26%
Other not listed	7%

% respondents (46)

7. Organisations generally comply at least partially with industry standards designed to ensure good practice in the areas of Information Security. Whilst the Data Protections Act was widely adopted, this was not the case for other standards such as ISO/IEC17799, BS7799 Pt 2 which are the main management standards, or ISO 1900. There was little knowledge of ACPO Guidelines.

Which of the following industry standards does your system comply with?

Legend: Fully comply / Partially comply / Not comply / Don't know/N/A

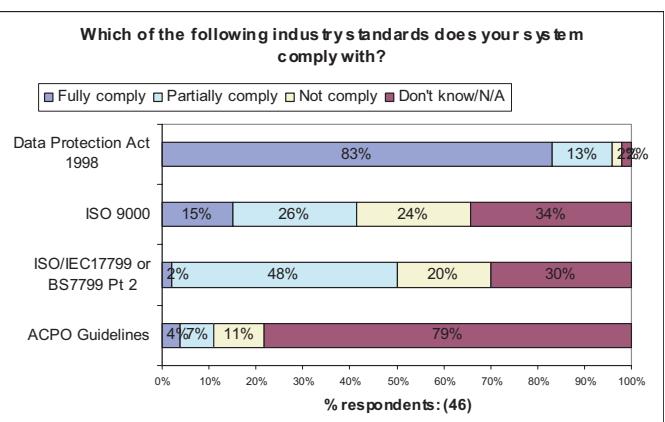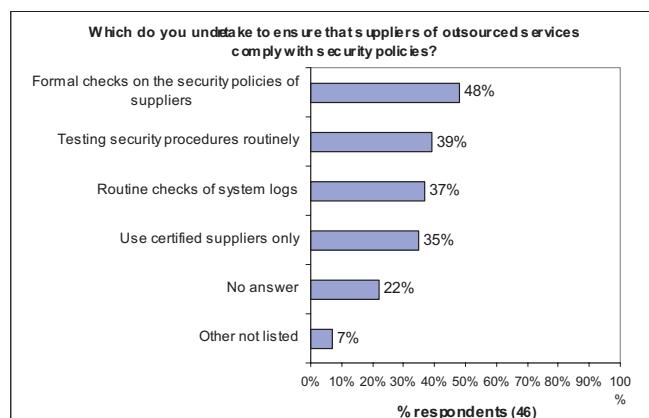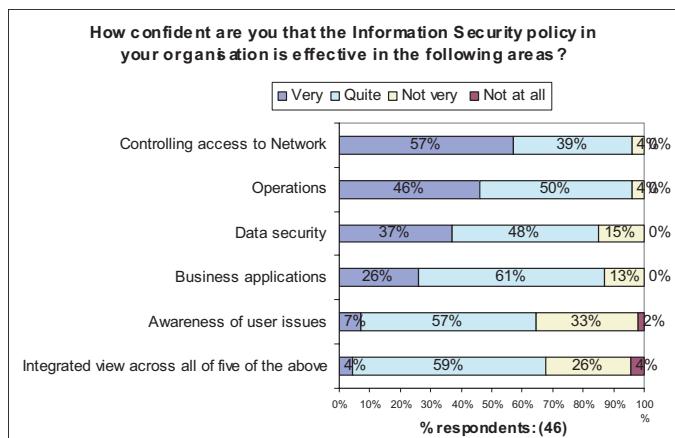|	Fully comply	Partially comply	Not comply	Don't know/N/A
Data Protection Act 1998	83%	13%	2%	2%
ISO 9000	15%	26%	24%	34%
ISO/IEC17799 or BS7799 Pt 2	2%	48%	20%	30%
ACPO Guidelines	4%	7%	11%	79%

% respondents: (46)

8. Most companies (74%) took some precautions in their use of any outsourced services but the figures did not indicate all measures were widely adopted. (22% did not answer this question implying that no outsourced services were used.)

81% of those answering the question did some form of vetting of their suppliers, making formal checks on the security policies of their suppliers or using only certified suppliers. 66% undertook controls at the system end either by routinely testing their security procedures or running checks of their logs.

Which do you undertake to ensure that suppliers of outsourced services comply with security policies?

Formal checks on the security policies of suppliers	48%
Testing security procedures routinely	39%
Routine checks of system logs	37%
Use certified suppliers only	35%
No answer	22%
Other not listed	7%

% respondents (46)

9. Supporting the findings from point 5, few companies demonstrated real lack of confidence in their Information Security Policy. Most respondents indicated confidence in the control of their networks, their operations and data security. Any lack of confidence in their policies was concerned with 'awareness of user issues' and how integrated their approach was on their security policy.

How confident are you that the Information Security policy in your organisation is effective in the following areas?

Legend: Very / Quite / Not very / Not at all

	Very	Quite	Not very	Not at all
Controlling access to Network	57%	39%	4%	0%
Operations	46%	50%	4%	0%
Data security	37%	48%	15%	0%
Business applications	26%	61%	13%	0%
Awareness of user issues	7%	57%	33%	2%
Integrated view across all of five of the above	4%	59%	26%	4%

% respondents: (46)

The Board Viewpoint

10. The Boards of Directors within organisations are perceived as having quite widely varying interest in the issue of Information Security. Whilst a third have a proactive interest, 43% are perceived as having a reactive interest and a quarter little or no interest at all.

Those who take a proactive interest do so because of the importance they attach to Information Security and the higher awareness or appreciation of the risk to their business. In some instances, this may be because their type of business is one where they have more to lose if security was compromised.

What is the attitude of the Board of Directors in your company to Information Security within your organisation?

Proactive interest	33%
Reactive interest	43%
Little or no interest	24%

% respondents (46)
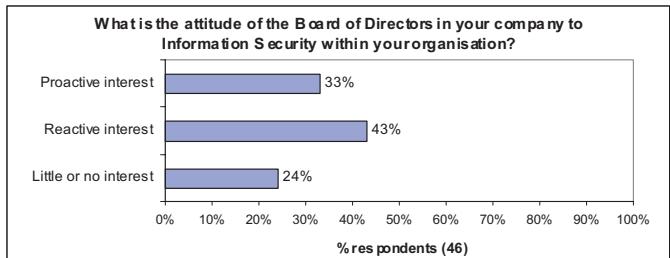
'This issue has always been on our agenda. It is not the value of the information assets but the impact on public confidence if our integrity were compromised.'

'Recognition that security is integral to our competitive advantage.'

'Information security is one of many areas of risk where the board has actively promoted risk analysis.'

The lack of interest of boards tended to be attributed to their lack of experience or appreciation of the potential risks and their priority with revenue-making sections of the business. This, coupled with the view that Security is an IT operational concern rather than a corporate one, reinforces the detached view that many Boards adopt. Their type of business may determine the level of importance and therefore interest in this issue.

'No first hand experience of major incidents.'

'Not viewed as a corporate priority, IT expected to deal with these issues.'

'Board are primarily interested in profit from the company. They view IT as something that happens which they don't need to know about, and they have minimal understanding.'

'Operational issue - day to day - just needs taking away and sorting, doesn't it?'

'The Culture of the business is such that they are not too concerned. We are a service industry and a lot of the market edge is from personal knowledge which is not on a computer.'

11. Boards tend to be detached from the issue of Information Security with updates on policy and investment carried out in four out of five cases either on an annual or even less frequent basis. A third either 'hardly ever or never' do so. Whilst over a quarter of respondents indicated they report security lapses to their boards on a monthly basis, over

How often do you update the Board on Information Security on the following?

Legend: Monthly, Quarterly, Annually, Hardly ever/never

	Monthly	Quarterly	Annually	Hardly ever/never
Security lapses	28%	15%	9%	43%
Security investment	2%	15%	43%	35%
Policy update	0%	20%	48%	33%

% respondents : (46)

40% hardly ever or never do so. These results would indicate that Information Security is not an issue in which Boards are having a significant level of dialogue.

12. The findings suggest that those organisations with more proactive boards seem to address the potential risks for Information Security more comprehensively than those Boards who take a more reactive or little interest in the issue of IS. Respondents with more proactive boards:
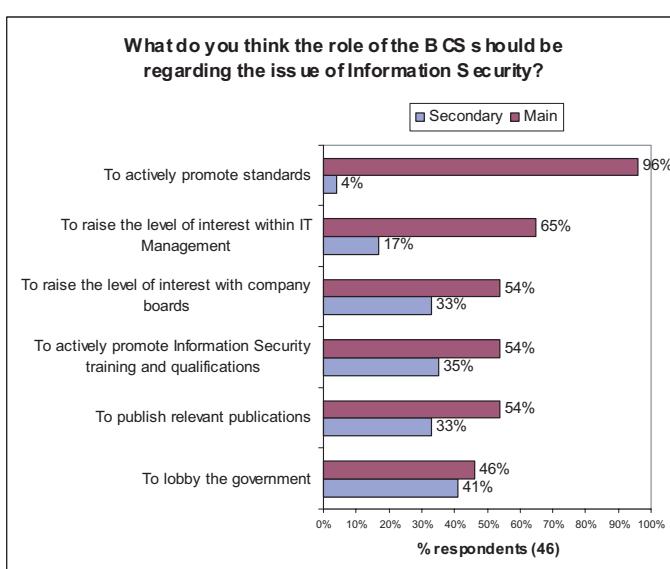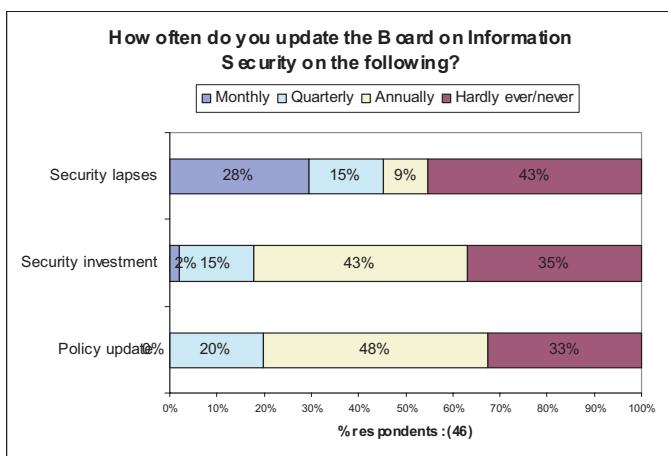
● Were in organisations more likely to have formalised plans in place to minimise the impact of their systems being damaged or compromised by unexpected events e.g. bomb threats, fire, virus attack, password breach.

● Were more likely to comply with industry standards such as as ISO/IEC17799, BS7799 Pt 2, ISO 1900 or ACPO Guidelines.

● Demonstrated a higher level of confidence in the efficacy of their Security policy, presumably as a result of these measures.

● Had more frequent communication with their Boards on Information Security, particularly on any security lapses.

Whilst the nature of the organisation's business will impact on the level of commitment to investment in Information Security, it can also be questioned whether the interest of the Board sets the agenda and is a key factor in determining the priority Information Security is given within the organisation.

THE BCS ROLE

13. The response to the potential role of the BCS would clearly confirm that Information Security is an issue which warrants a higher industry profile and the BCS is seen as having an active role to play on this. Some work is already being carried out in this area by the BCS Information Security Specialist Group.

Virtually all respondents felt that the remit of the BCS should be the active promotion of standards. This should be achieved by the promotion of training and qualifications in the Information Security sector as well as raising interest in this issue both with Boards and within the industry.

What do you think the role of the BCS should be regarding the issue of Information Security?

Legend: Secondary, Main

	Secondary	Main
To actively promote standards	4%	96%
To raise the level of interest within IT Management	17%	65%
To raise the level of interest with company boards	33%	54%
To actively promote Information Security training and qualifications	35%	54%
To publish relevant publications	33%	54%
To lobby the government	41%	46%

% respondents (46)

Dr Sharm Manwani held European IT Director positions at two multinational organisations while obtaining his MBA and Doctorate at Henley Management College. In 2000, he joined the faculty at Henley where he is researching, mentoring, and lecturing in Information Management. Dr Manwani is a founder member of the BCS Management Forum and consults with leading companies in Strategy and Programme management.

Sharmm@henleymc.ac.uk.

Caroline Fraser is Marketing Research Manager at The British Computer Society and has worked for a number of years in market research in both the publishing and education & training fields.

Cfraser@hq.bcs.org.uk

Acknowledgements

Australian Computer Crime and Security Survey 2003

Bob Ashton

The survey has recently been published for 2003. This year's was produced by the Australian Federal Police, Queensland Police, South Australia Police, Western Australia Police and AusCERT, whereas last year's survey was produced by AusCERT, Deloitte Touche Tohmatsu and NSW Police. See Spring 2003 issue.

The survey was adapted from the CSI/FBI Computer Crime and Security Survey, as last year, in order to facilitate easy comparison between Australia and the United States.

The total number of incidents has fallen from last year, and optimists could conclude that this was due to more effective counter measures having been taken by responding organizations. A more likely explanation is the more rigorous definition of "incident" in this year's survey. The fact that total losses have doubled over the previous year is worrying. Financial fraud, laptop theft and virus, worm and trojan infections were found to be the largest source of computer crime losses.

The observed trend of a shift towards a greater incidence of externally sourced harmful attacks over internal has continued. Despite high use of anti-virus software and policies for developing controls against malicious software, 80% were infected with a virus, worm or trojan and 57% suffered a financial loss as a result - more than last year.

The survey describes some decided court cases in the area of computer crime. Australian law now provides for severe penalties for computer crime. For example, Section 308D of the NSW Crimes Act provides for a penalty of 10 years imprisonment for "unauthorized modification of data offences". In view of the pathetic nature of the penalties actually imposed, this is unlikely to act as a deterrent.

The survey is available from: **www.auscert.org/**

17799 Checklist

After a long period of gestation, ISO 17799 is rapidly becoming the world-wide standard for information systems security. First promulgated as the Department of Trade and Industry Code of Practice, and renamed as British Standard 7799 in February 1999, the Standard was subject to a major revision and adopted by International Organization for Standardisation (ISO) as the "Code of Practices for Information Technology Management," in August 2000. The great advantage of this development is that a common framework now exists for organizations throughout the world to claim a mutually intelligible security standard to provide business confidence.

As a result many organizations may wish to assess their conformance status in respect of the Standard. Such a gap analysis process can be used as a precursor to certification under BS 7799.2:2002, or can be an end in itself. Certification can be a bureaucratic and costly exercise similar to compliance with ISO 9001. Auditors, however, can play a very useful role in providing their employing organizations with an assurance that their information security arrangements conform to best practice. At the same time the auditor will have provided him or herself with a comprehensive overview of the organisation's information security status and have established a sound basis for an information security audit plan.

A number of resources are available to assist in this. **Annex A of BS 7799.2:2002** consists of the control objectives and controls from ISO 17799, and has proven to be the most useful basis for a check list for reviewing conformance with 17799. The Australian Government's **I-RAP System Review Guidelines & Checklist (v.1.2)** is even more useful as it also contains best practice recommendations. These best practice recommendations are cross referenced to the Australian Communications-Electronic Security Instructions 33 (ACSI 33).

ACSI 33 is a series of publications, known as handbooks, produced by the Defence Signals Directorate (DSD) - the Australian equivalent of GCHQ, to provide guidance to Australian Government agencies wishing to protect their information systems. Each handbook covers a specific topic:

1. Standards
2. Evaluated Products
3. Risk Management
4. Security Management
5. Emanations and Cabling Security
6. Media Security
7. System Access Control
8. Network Security
9. Cryptographic Systems
10. Web Security
11. Email Security
12. Malicious Software
13. Intrusion Detection
14. Physical Security

Each of these handbooks is a valuable resource for the subject it addresses, and together go a long way to providing a comprehensive resource for addressing the issues raised by 17799.

Each handbook discusses the relevant security issues and, where appropriate, categorises countermeasures into appropriate risk levels, together with appropriate recommendations.

ACSI 33 has been written to be consistent with ISO 17799 and Australian Standard AS/NZS 4360 - Risk Management. Although this advice contained has been provided for Australian Commonwealth Government agencies and the Australian Defence Force, it contains a mine of valuable advice which can be accessed by everyone. Although not as voluminous as the German Federal Government's IT Baseline Protection Manual, ACSI 33 covers some areas not addressed by that document.

As the **I-RAP System Review Guidelines & Checklist (v.1.2)** is structured and ordered exactly as 17799 it is of great value to an auditor looking for guidance in this area.

All the above Australian documents are available from **www.irap.standards.com.au**

The Price of Stupidity

Bob Ashton

Stories such as the one that follows were common 30 years ago. That fact that they can still happen erodes one's faith in human progress.

What a world? .... On Thursday, 24 January 2002, Derek Guille broadcast this story on his afternoon program on ABC radio. (Australia). In March, 1999, a man living in Kandos (near Mudgee in NSW) received a bill for his as yet unused gas line stating that he owed $0.00. He ignored it and threw it away. In April he received another bill and threw that one away too. The following month the gas company sent him a very nasty note stating they were going to cancel his gas line if he didn't send them $0.00 by return mail. He called them, talked to them, and they said it was a computer error and they would take care of it. The following month he decided that it was about time that he tried out the troublesome gas line figuring that if there was usage on the account it would put an end to this ridiculous predicament. However, when he went to use the gas, it had been cut off. He called the gas company who apologised for the computer error once again and said that they would take care of it. The next day he got a bill for $0.00 stating that payment was now overdue. Assuming that having spoken to them the previous day the latest bill was yet another mistake, so he ignored it, trusting that the company would be as good as their word and sort the problem out. The next month he got a bill for $0.00. This bill also stated that he had 10 days to pay his account or the company would have to take steps to recover the debt. Finally, giving in, he thought he would beat the company at their own game and mailed them a cheque for $0.00. The computer duly processed his account and returned a statement to the effect that he now owed the gas company nothing at all. A week later, the manager of the Mudgee branch of one of Australia's major banks called our hapless friend and asked him what he was doing writing a cheque for $0.00. After a lengthy explanation the bank manager replied that the $0.00 cheque had caused their cheque processing software to fail. The bank could therefore not process ANY cheques they had received from ANY of their customers that day because the cheque for $0.00 had caused the computer to crash. The following month the man received a letter from the gas company claiming that his cheque has bounced and that he now owed them $0.00 and unless he sent a cheque by return mail they would take immediate steps to recover the debt. At this point, the man decided to file a debt harassment claim against the gas company. It took him nearly 2 hours to convince the clerks at the local courthouse that he was not joking. They subsequently assisted him in the drafting of statements which were considered substantive evidence of the aggravation and difficulties he had been forced to endure during this debacle. The matter was heard in the Magistrate's Court in Mudgee and the outcome was this: The gas company was ordered to:

1. Immediately rectify their computerised accounts system or show cause, within 10 days, why the matter should not be referred to a higher court for consideration under company Law.

2. Pay the bank dishonour fees incurred by the man.

3. Pay the bank dishonour fees incurred by all the bank's clients whose cheques had been bounced on the day our friend's had been.

4. Pay the claimant's court costs; and

5. Pay the claimant a total of $1500 per month for the 5 month period March to July inclusive as compensation for the aggravation they had caused their client to suffer.

And all this over $0.00.

Annual General Meeting

May 13th 2003

Chairman's report

We have held six successful meetings so far this year, and have survived an ongoing crisis in participation by members in the work of your management committee.

The meetings in the 2002/3 programme ending today were:

1. Database Security in October (late afternoon, 39 attended)
2. Implementing and Auditing IT Governance in November (a full day with and at the ICAEW, 56 attended)
3. BS 7799 in December (late afternoon, 38 attended)
4. Cybercrime Uncovered in January (full day, 22 attended)
5. Digital Signatures in February (late afternoon, 31 attended)
6. Systems Development and Auditing in March (full day, 22 attended), and
7. Hackers (later on today, 32 booked to attend).

The late afternoon format seems to have become more popular, possibly because of the relatively costly free buffet that concludes it and the excellent opportunity for "networking" thereby provided!

The SG has not functioned as efficiently as it should do, for a variety of reasons, primarily because there were not enough active management committee members. It may also be that fewer people are now active in computer audit and related information risk management roles.

My own position may have contributed to this unsatisfactory state of affairs. Following my wife's prolonged illness and then death in February last year, my own health deteriorated somewhat, leaving me with too little energy either to work or to be an active SG chairman. However my health has improved and I feel considerably more energetic now. I may return to work shortly, perhaps in computer audit and related information risk management roles, perhaps in general IT consulting, or I may retire to the south of France. Following several encouraging press reports I did briefly consider a late career as a well-paid London plumber. However I have not yet decided what to do.

We can be more positive about the future because a number of volunteers have now come forward to join the committee and to become Treasurer.

I would like Alex Brewer, a committee member who recently gave us the excellent talk on database security, to act as deputy chairman in future, with the prospect of becoming the next SG chairman. I have been chairman for many years, but have not worked in a computer audit or related information risk management role since 1999. It is time for a change, but we need to give Alex the chance to "settle in" gently. Alex works in information security at Lloyds TSB Bank.

Largely in response to a strongly worded appeal I sent to all members, with the last issue of the Journal, four members and a speaker have volunteered to join the committee. Another member (Jean Morgan) has volunteered to take over from our retiring Treasurer. When we come to elections I shall tell you a little about these volunteers. With enough people the work of managing the group effectively can be split into smaller and more acceptable parts, so I am optimistic about the group functioning more efficiently next year.

Later on today you will see what meetings we are proposing for next year. The draft programme is on your chairs. We would appreciate receiving your feedback, suggestions for speakers, and other ideas.

I should like to thank our outgoing Treasurer Jan Lubbe for his sterling efforts and wish him well in his career outside computer audit and information risk management. I should also like to thank Siobhan Tracey in her role as Secretary and meeting organiser. I must thank those others on the committee who have stayed with us through these difficult times, and in particular: John Mitchell who edits the Journal, Allan Boardman our webmaster, and Celeste Rush. Thanks are due also to Janet Cardell-Williams our administrator, and to KPMG which provides the venue for this and other later afternoon IRMA meetings free of charge.

Meet Some of Your Committee

Alex Brewer

(Deputy Chairman)

I studied piano at City University and the Guildhall School of Music and Drama. A strange beginning for someone involved in information risk management, but in hindsight, an inspired choice. All systems audit professionals know that what computers really get up to is invisible, and in trying to unearth the processes and controls you are dealing with objects which are descriptions of the process, but which are not the process itself. This is similar to the process of building a musical performance! I subsequently trained as a Chartered Accountant, moving to systems audit work in 1990 at KPMG following qualification. As well as working for a diverse portfolio of clients I also qualified as a CISA which at that time was one of the key audit and security qualifications. I left in 1995 to work for the Lloyds TSB Group and the Mitsubishi Trust and Banking Corporation, both as a systems auditor and in information security. My current

On Red Nose Day I have been known to cart my guitar into work to raise money. This year I persuaded people to part with £280.

job is as an auditor in Morgan Stanley.

My agenda in the audit and security space is to encourage the addressing of database security issues, which are often ignored in the rush to implement firewalls, intrusion detection and other fashionable technology. The databases,

meanwhile, have lumbered on, their security unseen by most audit and security professionals. For IRMA I see my agenda as enabling the committee to continue the excellent training for others, which I have taken in the past for my own continuing professional education, as well as trying to grow the (people)

networking aspects of the group.

If you would like to discuss any of this or other IRMA matter with me you will find my contact details on page 19 of this Journal.

Jean Morgan (Treasurer)

I have taken over as Treasurer for the group. My background is in systems development and project and programme management. I have been working as a freelance IT Management Consultant for six years and I also do project audits and project reviews, as well as IT Due Diligence for both procurements and for funding decisions. So how did I get involved with IRMA? Well, I am a BCS Member and have been active with PROMS-G (Project Management Specialist Group) for several years - I was Treasurer for four years until this January. Through the BCS, I heard about and attended several of IRMA's day seminars over the years and found them to be excellent value for money and covering such a broad range of topics. When I heard that the group might fold for lack of a committee I was disappointed. So my conscience, and

the fact that I'd done BCS treasuring for years so low learning curve, persuaded me to offer my services to the group. I'm glad that others also boosted the membership of the group and I hope that we will continue to grow and prosper. By the way, for similar reasons, I am also treasurer for the new BCSWomen specialist group.

As a permanent employee and as a consultant, I have worked in financial services (banks and insurance companies) and also in defence engineering and central government. I am based near Fordingbridge, close to the borders of Hampshire, Wiltshire and Dorset. But I am finding that these days I have to travel further and further from my home/ office for work. I have a husband and a teenage son. We are keen rugby fans - of Gloucester, my husband's home town, and of my son's school and club teams. We are also keen environmentalists so I'll be the one picking up cans and bottles to recycle at the next seminar (if I can carry them!). There are some potentially more interesting photos of me on my web site, **www.wilhen.co.uk**, from the Moonwalk - I recently walked a marathon around London with 15,000 others through the night of 10th May.

Graham Devine (Events)

I have a confession; I am not an Information Systems auditor. In fact I am not any kind of auditor. So now that you all know my terrible secret 'what.......', I hear you ask, '......is this...this...this OUTSIDER doing on the IRMA committee?''.

Well, I have two key motives for my infiltration of FORTRESS IRMA!

Firstly - in my 25 years of professional assignments in IT/IS Service Delivery, Business Systems Development and Project Management, I have constantly needed to address subjects which I know to be central to the IS Audit 'domain'. Such things as:

● Operational and Project Risk

● Access control and data security

● Internal Control policy and practice

● Governance

● Business Continuity

Past roles have seen me delivering new business systems and earnestly trying to balance the (apparently

opposed) 'needs' of business, common sense, policy, audit and legislation. More recently I have enjoyed the challenges of: embedding IS Internal Control in an International Vehicle Leasing company, promoting and developing Business Continuity/Disaster Recovery plans and performing Year 2000 preparedness reviews upon unwilling facilities and IT departments. Hopefully you can now see that, although I am not part of the qualified audit 'club', nevertheless I have experience relevant to 'the cause'.

Secondly I want to learn and I want to help. I have spent the last 5 years or so following my own courses of professional development; the BCS through its branches and special interest groups has been at the core of this and I think it is time to give something back. Also, I am at a turning point in my career and I am not too big headed to think that at the ripe old age of 44 I can still learn something from the committee, members and other 'experts' in IRMA.

So what is my role in IRMA? Well I am one half of the EVENTS PROGRAMME MANAGEMENT team -

Raghu Iyer is my more experienced and 'better' half. What do we hope to achieve?

● Create an outstanding programme of free and low cost/high value events for the coming year. Well we seem to have go off to a good start - you will see from elsewhere in the journal that we have already planned an event for each month from October 2003 through to May 2004. Most of these have dates and organisers/speakers arranged - make sure you block these out in your diary!

- Focus (this means cajole and harass!) our volunteer organisers and speakers on getting their specific event days planned, resourced, published and executed effectively.
- Attract a greater number of attendees to IRMA events. We wish to broaden the appeal and increase the membership of IRMA - better

publicity and more relevant and valuable event content will help.
- Promote liaison between IRMA and related professional groups (e.g. ICAEW, IIA, ISACA, BCS-ISSG etc.). We hope also to increase cross-group attendance at events through reciprocal advertising and the maintenance and extension of attractive entry rights.

- Begin planning the events for the 2004-2005 programme early. If you have any ideas for subjects you would like to see covered or maybe want to run an event yourself please drop a note to Raghu and myself.

My last motive is to enjoy myself!

I hope to see you at all of the IRMA events from October onwards.

Ross Palmer
(External Relations)

As a new member of the IRMA Management Committee, I'd like to say "Hello there", rather than the trite "Hi" you hear every week from University Challenge contestants. (This, of course, immediately identifies two great passions of mine: (a) staunch defender of the English language, and (b) connoisseur (failed) of the cultural general knowledge quiz.). My specific function on the committee is "External Liaison", a role that I see as evolutionary rather than defined, but which broadly encompasses establishing and developing relations with other professional organisations having similar objectives for their members.

I want to establish personal contacts within these organisations by any means at my disposal - website searches; cold calling; networking at seminars; etc - and I would welcome suggestions and references from the wider IRMA membership as to suitable knowledge-sharing partnerships. Such relationships, if developed carefully, can lead to mutual benefits by acquiring and sharing

professional knowledge to enhance audit, control and risk management practices among memberships. This can also optimise seminars and other presentations, avoiding undesirable clashes of dates and topics, with mutually preferential terms negotiated.

So, what else about me could possibly interest you? I am 53 years old, MIIA and CISA-qualified, and have been in and out of computer audit and risk management for more years than I care to remember, having spent what some may consider a lifetime (23 years) working for the Department of Health

and Social Security, followed by 10 years in the banking world and 2 more (to date) as Computer Audit Manager for Hogg Robinson plc. My principal hobby is my guitar, or, rather, my 5 guitars (6-string and 12-string acoustics, soft and hard-strung classicals and a Fender Stratocaster), which, over the decades have brought me much pleasure and stress-relief but little income. I fronted a heavy rock band in the 70s (you wouldn't think so, looking at the mug-shot, would you?) and led a much quieter 80s and 90s playing and teaching classical guitar to unwilling children with over-eager parents.

How can music and internal audit co-exist and complement each other? (Sounds like an interesting seminar title.) Well, it would certainly spice up the Powerpoints and a modicum of audience participation would keep them alert during the graveyard shift after lunch. My favourite audit song is "They're Coming To Take Me Away, Ha-Haaa". On one notable occasion, some colleagues and I presented a musical, satirical opener for the NatWest Audit Conference. Ask Paul Plane - he was one of those singled out, but he took it well.

Mark Smith
(IIA & NHS Liaison)

Having joined the IRMA Committee in April, I thought it would be useful to give members some background information about myself and how I plan to assist in the management of IRMA. After leaving school in 1993, I joined Suffolk County Council as an in Internal Audit trainee. I went on to spend five years there, during which time I achieved a BTEC Advanced Business Studies award and the Association of Accounting Technicians (AAT) qualification.

In 1998 I joined the NHS, working for

my current employer: Suffolk Audit Services. For the first couple of years most of my workload was financial auditing. However, because of the

imminent retirement of our current Computer Audit Consultant and my interest in IT, I agreed a Computer Auditor development plan with our Director in 2001 and promptly enrolled on the Institute of Internal Auditor's (IIA) Qualification in Computer Audit (QiCA). I am now part-qualified in this and need to pass one more exam to achieve the academic part. However, there is also a requirement to undertake 1,600 hours IT audit covering specific areas, which I am some way off achieving as yet. Next year, I intend to enrol for the Certified Information Systems Auditor (CISA) qualification, as I am aware this is a qualification highly respected internationally.

As well as being interested in computing, I enjoy travelling. This year I have visited Belgium, France and my wife's home country: Estonia. Estonia has been independent since 1991 and I am not sure they have any Computer Auditors as yet, that's something I would be interested to look into! I am interested in current affairs and politics, especially environmental and humanitarian issues. I am a member of organisations including Climate Care, Oxfam, the RSPB, the Woodland Trust and WWF-UK. My other interests include visiting the theatre and cinema, and going to football (Ipswich Town FC). Because of my knowledge of the NHS and the IIA, I have agreed to play a liaison role between these organisations and IRMA. I am confident that I can find many new members as, like myself until recently, I suspect many Computer Auditors have either not heard of IRMA or not properly considered the benefits

of joining. IRMA is a wonderful training and networking resource that I would like to be made us much use of as possible.

The NHS (**www.nhs.uk**) employs over a million people and has an annual budget of more than fifty billion pounds. It is audited by a variety of internal and external audit providers. Internal Audit is regularly market tested, resulting in services being provided typically by private firms or NHS-employed consortia (such as Suffolk Audit Services). I have obtained contact details for approximately 120 Heads of Internal Audit and intend to write to them all to explain the benefits that IRMA has had to me and how their Computer Auditor(s) would also benefit from joining. I will give basic details of forthcoming events and request they contact to me if interested. I will then arrange for a copy of the IRMA magazine

and a joining form to be sent to them.

The IIA (**www.iia.org.uk**) has around 75,000 members world wide of which over 6,000 are based in the UK. They offer three qualifications: PIIA (Practitioner), MIIA (Member) and QiCA (Computer Audit). IRMA should be of interest to QiCA qualified auditors and would be hugely valuable for QiCA students, so I am keen to explore avenues to promote IRMA to the IIA (and vice versa). IRMA members may be interested to note that the IIA has an Information Security Special Interest group, see **www.issig.org.uk**

Please don't hesitate to contact me regarding IRMA, the NHS, the IIA, Ipswich Town's promotion push, computer audit in general.......my contact details can be found on page 19 of this Journal.
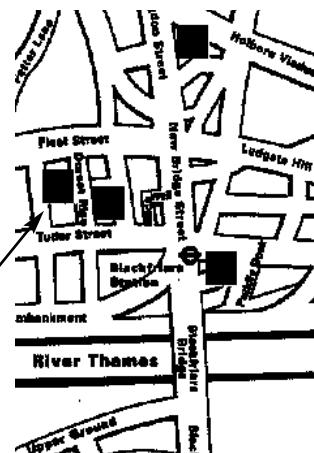

Venue for
Full Day Briefings

Old Sessions House
Clerkenwell Green
London EC1

KPMG
8 Salisbury Square
London EC4

Venue for
Late Afternoon Meetings

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 my column at the end of 2002, I outlined plans to seek Privy Council approval for changes to the BCS Royal Charter affecting both the governance arrangements and the membership structure of the Society. At that time, we expected to be ready to put proposals to an Extraordinary General Meeting (EGM) of members in the first half of the 2003. In the event, the process of finalising the proposals and consulting with other interested bodies took longer than anticipated but we are now ready to move forward and the EGM will take place on 23 September.

The proposed changes, as agreed by BCS Council, have three major elements - new Governance arrangements, a new membership structure and a new chartered title.

New Governance Arrangements

At the present time, the governance responsibility for the Society resides with Council, and each of the 45 members of Council is a trustee, responsible under Charity law for the actions of the Society. However, if current proposals are approved, these arrangements will change

* A new two-tier governance structure will be introduced, with a small executive board, to be named the Trustee Board, and a representative advisory new Council.
* The powers of governance of the Society currently vested in Council, except those for the election of the Trustee Board, will be vested in the Trustee Board.
* A new Council will be established, representative of the membership. Its primary role, apart from the

powers to elect members to the Trustee Board, will be advisory.

The Society believes that these arrangements will be better suited to its current needs. The Society is now a medium sized business with a £15m turnover, and growing. We have to make ourselves more business-orientated and make the right decisions quickly. Under the new arrangements, a smaller Board of Trustees, meeting much more frequently than existing Council, will be more closely engaged with the day to day business of the BCS.

New membership Structure

The aim of the new membership structure, to be put to members for decision on 23 September, is to make BCS membership more easily accessible to all competent professionals through a new rapid application process. The new arrangements will also provide access to professional membership at a very much earlier career stage for the best of the young professionals.

The aim is to achieve that without reducing standards or threatening the

Colin Thompson
BCS Deputy Chief Executive

link with the Engineering Council. How? - Quite simply by adopting a two stage approach to professional membership. Chartered status will be separated from professional membership so that candidates can enter the professional grades, as a stepping-stone to chartered status, much earlier in their career - and through a greatly simplified admission process. Chartered status will be protected - and promoted - as the "gold standard' of our membership structure and the more rigorous processes will be retained. The resulting structure is shown in the diagram below:

For those with the most relevant academic qualifications - including BCS professional examinations and BCS-accredited university degrees, the new arrangements will provide access to MBCS at the point of graduation. Those with lesser academic qualifications, or
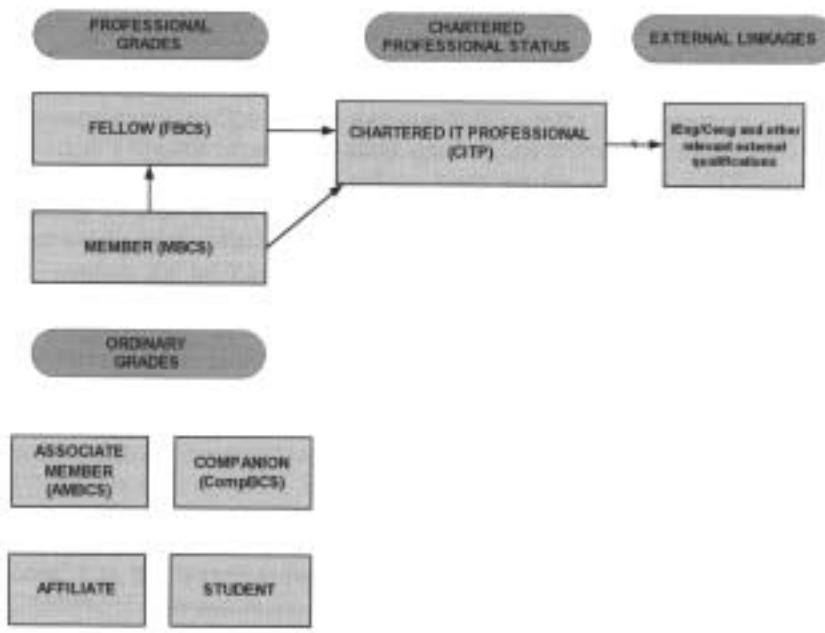
with no academic qualifications at all will need between 2 and 5 years experience. For all candidates, the aim is to provide a process that delivers entry to professional membership within a matter of days rather than weeks or months.

A New Chartered Title

Professional members who achieve Chartered Status will be entitled to use a new chartered title - *Chartered IT Professional,* with the post nominal letters CITP. All existing Members and Fellows will, of course, take this new title immediately the new charter comes into effect.

The 23rd September Vote

Overall, these proposals are intended to provide the foundation for a Society which is more representative of the professional community and more relevant, not only to the professionals within that community but also to their employers and customers. These changes can however only be made with the approval of the voting members and, subsequently, the Privy Council. Within the BCS, Members (MBCS) and Fellows (FBCS) make up the voting constituency and, under current rules, Charter changes require a 75% majority of those voting.

Following the EGM, assuming that the vote is positive, the application will be referred to the Privy Council. Preliminary consultation indicates that this application is likely to be successful and, in that event, the changes will be introduced on 1 May next year, in time to recruit the 2004 graduating class.

The Case for an IT profession

Simply making BCS professional qualifications more readily available will not, of itself, strengthen the case for an IT profession; that can only come from a much greater recognition of the value of such qualifications in the market place. In particular it requires employers to attach greater value to professional qualifications in their recruitment and personnel policies. It was with this in mind that BCS set up a working party earlier this year, with representation from the IEE and from IBM, to examine the relationship between professionalism and performance in the delivery of ICT products and services.

That working party has made some considerable progress in identifying the issues and in building the case for professionalism - including but not limited to the professionalism of IT staff - as the solution to the problems of quality. We are now in discussion with a number of other major IT organisations and with government on these issues and it is clear that there is a very real interest in building a much more professional approach to the delivery of IT products and services.

Possibly - just possibly - a recognised IT profession is an idea whose time has come. If so, the changes to the BCS membership structure and the launch of the Chartered IT Professional title are very timely.

A FIFTH BIRTHDAY CELEBRATION FOR ECDL

The European Computer Driving Licence is 5 years old. The internationally recognised user qualification was launched in the UK by the BCS in May 1998 to address the divide between the arrival of new technology and people's ability to use it effectively.

And what an exciting 5 years the qualification has had. In the first year there were just 1,200 candidates and 150 test centres, but from there on, take up has exceeded all expectations and there are now 2500 test centres and over 600,000 registered individuals in the UK alone. BCS is on target to reach 1m registrations by the end of the year.

Individuals of all ages have achieved the ECDL, the vast majority using it in their work and to enhance the career prospects.

Major employers have also adopted the qualification, including IBM, the National Health Service, the Bank of England, J Sainsbury, HSBC and Pfizer. The Cabinet Office is also offering staff across the Civil Service the chance to gain the qualification as part of the government's drive to deliver all services electronically by 2005.

A NEW PRODUCTS AND SERVICES BOARD

One more step on the road to the BCS becoming a much more business-focused organisation was approved by the Policy and Resources Committee recently. A new Board is to be created, under the Chairmanship of the Honorary Treasurer, to take responsibility for all BCS products and services, particularly those offered on a commercial basis. This will include the BCS professional examinations, ISEB qualifications, ECDL and the commercial publishing activity of the Society. The new Board will have responsibility principally for the commercial aspects of the products and services; issues relating to content - for example the syllabus for the exams, will reside elsewhere.

This move supplements others over the past year towards a more business-focused approach, including the creation of a new Business Planning Unit and the introduction of a comprehensive Gateway process to govern the appraisal of all investment decisions relating to new, or existing, products and services.

And finally...........

Two BCS events for the diary - the AGM on the 23rd October and the Annual Dinner on 20th November. The AGM, exactly one month after the EGM on the 23rd September, will mark the start of the Presidency of Professor Wendy Hall. Wendy is only the second woman to reach the top position in the Society - Steve Shirley being the other. David Morriss, currently Vice President External Affairs will move into the Deputy President's seat, vacated by Wendy, and Brian Collins will replace David as Vice President.

Details of the venue and the speaker for the Dinner have yet to be confirmed but, given that this is Wendy's night, we can expect the event to be both different and special!

HUMOUR PAGE

What's in a word?

Each year the Washington Post's Style Invitational asks readers to take any word from the dictionary, alter it by adding, subtracting, or changing one letter and supply a new definition.

12) Intaxication: Euphoria at getting a tax refund, which lasts until you realize it was your money to start with.

11) Reintarnation: Coming back to life as a hillbilly.

10) Foreploy: Any misrepresentation about yourself for the purpose of getting laid.

9) Giraffiti: Vandalism spray-painted very, very high.

8) Sarchasm: The gulf between the author of sarcastic wit and the person who doesn't get it.

7) Inoculatte: To take coffee intravenously when you are running late.

6) Hipatitis: Terminal coolness.

5) Osteopornosis: A degenerate disease. (this one got extra credit)

4) Karmageddon: It's like, when everybody is sending off all these really bad vibes, right? And then, like, the Earth explodes and it's like, a serious bummer.

3) Glibido: All talk and no action.

2) Dopeler Effect: The tendency of stupid ideas to seem smarter when they come at you rapidly.

And, the pick of the lot:

1) Ignoranus: A person who's both stupid and an a**hole

Court Statements

These are things people actually said in court, word for word, taken down and now published by court reporters who had the torment of staying calm while these exchanges were actually taking place:

Q: What is your date of birth?
A: July fifteenth.
Q: What year?
A: Every year.

Q: What gear were you in at the moment of the impact?
A: Gucci sweats and Reeboks.

Q: This myasthenia gravis, does it affect your memory at all?
A: Yes.

Q: And in what ways does it affect your memory?
A: I forget.
Q: You forget. Can you give us an example of something that you've forgotten?

Q: How old is your son, the one living with you?
A: Thirty-eight or thirty-five, I can't remember which.
Q: How long has he lived with you?
A: Forty-five years.

Q: What was the first thing your husband said to you when he woke that morning?
A: He said, "Where am I, Cathy?"
Q: And why did that upset you?
A: My name is Susan.

Q: And where was the location of the accident?
A: Approximately milepost 499.
Q: And where is milepost 499?
A: Probably between milepost 498 and 500.

Q: Sir, what is your IQ?
A: Well, I can see pretty well, I think.

Q: Did you blow your horn or anything?
A: After the accident?
Q: Before the accident.
A: Sure, I played for ten years. I even went to school for it.

Q: Do you know if your daughter has ever been involved in voodoo or the occult?
A: We both do.
Q: Voodoo?
A: We do.
Q: You do?
A: Yes, voodoo.

Q: Trooper, when you stopped the defendant, were your red and blue lights flashing?
A: Yes.
Q: Did the defendant say anything when she got out of her car?
A: Yes, sir.
Q: What did she say?
A: What disco am I at?

Q: Now doctor, isn't it true that when a person dies in his sleep, he doesn't know about it until the next morning?

Q: The youngest son, the twenty-year old, how old is he?

Q: Were you present when your picture was taken?

Q: So the date of conception (of the baby) was August eighth?
A: Yes.
Q: And what were you doing at that time?

Q: She had three children, right?
A: Yes.
Q: How many were boys?
A: None.
Q: Were there any girls?

Q: You say the stairs went down to the basement?
A: Yes.
Q: And these stairs, did they go up also?

Q: How was your first marriage terminated?
A: By death.
Q: And by whose death was it terminated?

Q: Can you describe the individual?
A: He was about medium height and had a beard.
Q: Was this a male, or a female?

Q: Is your appearance here this morning pursuant to a deposition notice which I sent to your attorney?
A: No, this is how I dress when I go to work.

Q: Doctor, how many autopsies have you performed on dead people?
A: All my autopsies are performed on dead people.

Q: All your responses must be oral, OK? What school did you go to?
A: Oral.

Q: Do you recall the time that you examined the body?
A: The autopsy started around 8:30 p.m.
Q: And Mr. Dennington was dead at the time?
A: No, he was sitting on the table wondering why I was doing an autopsy.

Q: Are you qualified to give a urine sample?

Q: Doctor, before you performed the autopsy, did you check for a pulse?
A: No.
Q: Did you check for blood pressure?
A: No.
Q: Did you check for breathing?
A: No.
Q: So, then it is possible that the patient was alive when you began the autopsy?
A: No.
Q: How can you be so sure, Doctor?
A: Because his brain was sitting on my desk in a jar.
Q: But could the patient have still been alive nevertheless?
A: Yes, it is possible that he could have been alive and practising law somewhere.

Management Committee

CHAIRMAN	John Bevan	john_bevan@ntlworld.com
DEPUTY CHAIRMAN	Alex Brewer	alex.brewer@morganstanley.com
SECRETARY	Siobhan Tracey	siobhan.tracey@booker.co.uk
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Celeste Rush	rushlse97@aol.com
JOURNAL EDITOR & SECURITY PANEL LIAISON	John Mitchell	john@lhscontrol.com
EVENTS PROGRAMME MANAGER	Graham Devine	graham@grahamdevine.me.uk
EVENTS PROGRAMME CONSULTANT	Raghu Iyer	raguriyer@aol.com
LIAISON - IIA & NHS	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON - LOCAL AUTHORITY	Peter Murray	cass@peterm.demon.co.uk
LIAISON - ISACA	Ross Palmer	ross.palmer@hrplc.co.uk
MARKETING	Wally Robertson	williamr@bdq.com
ACADEMIC RELATIONS	David Chadwick	d.r.chadwick@greenwich.ac.uk
	David Lilburn Watson	dlwatson@bcrm.co.uk

SUPPORT SERVICES

ADMINISTRATION	Janet Cardell-Williams t: 01707 852384 f: 01707 646275	members.irma@bcs.org.uk janet@carliam.co.uk
WEBMASTER	Allan Boardman	allan@!internetworking4u.co.uk
LIAISON - KPMG	David Aurbrey-Jones	david.aubrey-jones@kpmg.co.uk

OR VISIT OUR WEBSITE AT   **www.bcs-irma.org**

BCS IRMA SPECIALIST GROUP ADVERTISING RATES (July 03)

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.co.uk
Website : www.bcs-irma.org
BCS IRMA Specialist Group Advertising Manager
Eva Nash   Tel: 01707 852384 & 07973 532358
E-mail : eva@nash141.freeserve.co.uk

IRMA
INFORMATION RISK MANAGEMENT & AUDIT

◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Membership Application
(Membership runs from July to the following June each year)

I wish to APPLY FOR membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 members) *   £75
   * Corporate members may nominate up to 4 additional recipients for
      direct mailing of the Journal *(see over)*

INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)*   £25

INDIVIDUAL MEMBERSHIP *(A members of the BCS)*   £15
BCS membership number: _____

STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment).
Educational Establishment: _____   £10

Please circle the appropriate subscription amount and complete the details below.

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS:
POST CODE:
TELEPHONE: (STD Code/Number/Extension)
E-mail:

PROFESSIONAL CATEGORY: (Please circle)
    1 = Internal Audit   4 = Academic
    2 = External Audit   5 = Full-Time Student
    3 = Data Processor   6 = Other (please specify)

SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS IRMA" AND RETURN WITH THIS FORM TO
Janet Cardell-Williams, IRMA Administrator, 49 Grangewood, Potters Bar, Herts EN6 1SL. Fax: 01707 646275

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:
1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:
1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:
1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:
1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

STOP PRESS

COMPSEC - £200 discount for IRMA members.

Mention your IRMA membership when booking.