ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 6 NUMBER 1 SUMMER 95

The British Computer Society

Technical Briefings for 1995/96

Wednesday 11th October 1995

Third Party Liaison: Business ally or potential risk?

Chairman: **Chris Hurford**, The Audit Commission

Speakers: **Mike Cullen**, Chairman BCS Independent Computer Contractors Specialist Group
Jeremy Holt, Chairman BCS Computer Law Specialist Group
Chrissie Bligh, Information Systems Manager, Cambridgeshire County Council
John Machin, KPMG

Organisers: Allan Brown - 01803 327874
Paul Howitt - 01992 644250

Tuesday 16th January 1996

Information Highways: The role of the traffic policeman

Chairman: **Lynn Lawton**, KPMG

Speakers: **Geoff Cox**, Micro Active
Dr Roger Wallis, City University
Trevor Williams, Clarke Whitehill
Tom Mulhall, Manager of Detective Operations, BT

Organisers: Geoff Wilson - 01962 733049
Jim Ewers - 01992 555328

Tuesday 16th April 1996

"Readiness is All": Making better use of the Technology

Chairman: **Judith Scott**, Chief Executivet BCS

Speakers: **Graham Clukas**, Price Waterhouse
John Ford, Quality Methods Manager (IT), Safeway Stores plc
Sue Mathews, Training by Design
Stan Dormer, System Security Ltd.

Organisers: John Bevan - 01992 582439
Diane Skinner - 0117 923 6757

Tuesday 16th April 1996 16.30

ANNUAL GENERAL MEETING

Technical Briefings are held at the Royal Aeronautical Society (see page 30).

For last minute confirmation contact the relevant organisers.

The Journal is the official publication of the Computer 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

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by Dodimead Ball, St Albans, Herts.

Editorial

A new volume, a new editor and the makings of a new editorial team, but the journal still looks pretty much the same. This is on the basis that if it 'ain't broke, don't fix it', something that a number of organisations who have gone along the downsizing route may now be wishing was on their family crest. There are two major initiatives however. The first is that there is now a separate column devoted to BCS matters. This column will be edited by Colin Thomson who is the BCS's Membership Director and the idea here is to show you how membership of the BCS can benefit you. Currently, only ten percent of our members belong to our parent organisation and we feel that one of the reasons for this is that you are unaware of what the BCS does on your behalf. We hope that this new column will at least provide you with some background to what is happening in the BCS arena. The second, is that we are now going to make more use of photographs in order to 'personalise' our contributors.

This edition has contributions dealing with the internet, safety critical systems and the changes to the IIA's QiCa qualification. This last item is of particular interest to me, as I have spent many years trying to convince the IIA that many of our membership were, in the past, effectively disbarred from sitting for QiCa due to the need to attend a course of study. At last the IIA have taken some note of this and have made some changes which will make it easier for our members to sit for the qualification. This does not mean that the examinations are any easier however! See David Bentley's article for a full briefing on the subject.

I also make a plea for help. You will notice that the editorial team has been restructured so that its members have specific responsibilities. I need additional people to become 'editors' of a couple of new columns that I would like to implement. As 'editor' of a particular column you do not necessarily have to write it, but simply ensure a flow of material. Think of the power this gives you. People approaching on bended knee with coffers of gold simply, to persuade you to let their name appear in print! I would particularly like to start hotel and restaurant watch columns. After all, we auditors travel around a bit, so a little help on the rest and recreation side would not go amiss. I also need someone to pro-actively run the advertising side. Ideally we would like to make the journal self-financing. Do I have any volunteers for these unpaid, but rewarding jobs? All you need to do is to prepare one column each quarter to receive the undying gratitude of the rest of the membership. Come along you people who moaned at me when I was chairman about the lack of content in the journal. Now is your chance to put your pen where your mouth was.

John Mitchell

COMPUTER APPLICATIONS SYSTEMS AUDIT WORKSHOP

Objectives

This workshop is intended to provide delegates with sufficient knowledge for them to be able to review, evaluate and audit the controls in the various computer based applications that they may encounter during their audit duties.

At the end of the course the participants will be able to:

- Identify the different types of computer environment that they may come across during their duties.
- Be aware of the differences in control commensurate with the various types of environment and computer application.
- Understand the requirement for controls, both internal and external, to the application that they are auditing.
- Adopt a methodical approach to assessing application control risks.
- Be able to evaluate the integrity, or otherwise, of application controls.
- Be able to conduct tests to evaluate the operational effectiveness of the controls.

Although the workshop concentrates on live applications the areas covered are also applicable to systems under development.

Who Should Attend

General and financial auditors with a limited understanding of information systems and recent entrants to computer audit who have not previously attended a structured course on application control and audit.

Course Programme

The workshop will consist of a mixture of lectures, case studies and exercises. The practical nature of the workshop is emphasised by the fact that every lecture is followed, or sometimes preceeded by a related case study or exercise. Delegates will be expected to undertake some evening work on the first day of the workshop.

Topics covered will be:

- The information systems environment
- Types of application
- Types of control
- Auditing batch applications
- Auditing real-time systems
- Use of computer assisted audit techniques
- Auditing for control

Date : **30 – 31 October 1995**

Venue: **Swallow Royal Hotel, Bristol**

Fee: **IIA & BCS CASG Members: £536 + VAT**

Non-members: **£630 + VAT**

Note: This workshop is fully residential

Contact: The Training Officer
Institute of Internal Auditors – UK
13 Abbeville Mews
88 Clapham Park Road
London SW4 7BX

Tel: 0171 498 0101
Fax: 0171 978 2492

Contents of the Journal

Chairman's Corner

Alison Webb

John Mitchell, our Chairman for the last seven years, decided not to stand for re-election at our last AGM on 10 May. We owe him an enormous debt. His firm but good-humoured leadership, his unfailing patience and his steady flow of new ideas have ensured the continued success of the group over that time.

I'm glad to say that John will be taking on a new venture, he will from now on, take on the editorship of the Journal.

John has always had a keen interest in the Journal. He sees it, in my opinion quite rightly, as a key service we provide to our members, particularly those who live and work out of London. In the last four years under Rob Melville it has developed almost beyond recognition, and is now a professional publication with a range of interesting and informative articles. I have no doubt that under John's hand it will go from strength to strength.

A change of government is always a good time to review policies: and we have decided this year to change the format of our meetings quite radically. We have felt for some time that our programme of evening meetings is not quite meeting requirements: people these days weigh very carefully the time involved in attending, and if they are based any distance from London, may feel time to attend sessions that are not immediately and directly useful cannot really be justified.

Next year, we will have no evening meetings or discussion groups.

We will be concentrating instead on three whole-day Technical Briefings. These will be at the Royal Aeronautical Society in London, starting at a time to accommodate people who have to travel some distance. You'll see the list of dates and topics elsewhere in the Journal and in the Programme Card.

Two more differences:

After some debate, we have decided to make a charge of £40.00 per day (members), and £140.00 per day for anyone else wanting to attend. This should make the days self-financing and so not penalise those who don't or can't come.

Finally, we want to make time in each day for you to share your knowledge with us. If you have some experience of an issue covered in a Briefing, consider giving a short (15 minutes) presentation as part of the day. Every aspiring auditor has to be able to communicate really well these days: so here's your chance to get some practice!

Guidelines for Potential Authors

The Journal publishes two types of article: refereed and invited. Refereed articles should be technically oriented and based on current or future issues related to information systems audit, security or control.This type of article will be reviewed by at least one member of the editorial panel (anonymously). If published, it will be identified as a refereed paper.

An invited article need not be technical or overly academic (even Computer Auditors have a sense of humour!). In fact it need not even be 'invited'. Submission without invitation is encouraged and although this may lead to severe sub-editing by the Editor, submission will virtually guarantee publication.

We also invite members to volunteer for book, product and course reviews (anonymously if required).

Why not call John Mitchell (Tel: 01707 851454, Email: jmitchell@lhs.win-uk.net) to discuss how you can get your name in print.

BCS Matters

Edited by Colin Thompson, BCS Membership Director, this new column brings you regular news of CASG's parent organisation.

New Chief Executive

The new Secretary General and Chief Executive of the British Computer Society is Judith Scott.

Most recently Judith was Managing Director of Gandalf Digital Communications Limited, the UK subsidiary of Canadian company Gandalf Technologies Inc. - where she had responsibility for Gandalf's operations outside North America. Gandalf designs and manufactures information networking equipment.

She has spent her working career in the information technology industry, with 21 years in Canada before being posted to the UK in 1987. She has been a member of Canada's Communications Research Advisory Board, the International Standards Organisation and is currently a Council member of the Canada-UK Chamber of Commerce.

A member of the Canadian Information Processing Society during her time in Canada, she has been a member of the BCS ELITE Group since 1991. She holds a BSc(Hons) in Mathematics from St Andrews University and a Post-graduate Diploma in Computer Science from Cambridge University.

David Mann, President of the BCS, said that he was extremely pleased with the number of strong candidates that had responded to the recruitment advertising and search process. "Judith Scott's combined experience as a senior business manager and Information Systems professional is considered very appropriate for leading the Society in the next stage of its development and growth.

Judith Scott

BCS - THE CASE FOR MEMBERSHIP

Colin Thompson

First the good news – membership of the BCS is currently growing steadily and over the past year the total number of members and applicants for membership has increased by approximately 2,000 to around 34,500. The bad news is, of course, that at that level we still represent a relatively small minority of those involved in the Information Systems business. Part of my task, as Membership Director for the Society, is to change that position and my immediate objective is to reach 40,000 members by the end of April 1996.

So what do I say to persuade non members to join? More specifically, in a world in which few employers demand professional qualifications or appear to give much weight to such qualifications in staff promotion, what advantage is there in belonging to the Society? Clearly I can produce a list of the direct benefits – publications, Branch and Specialist Group events, library and information services and the new BCSNet service for example. But that is only part of the story. No professional body would justify itself solely on the basis of the direct benefits of membership and that is particularly so for one in a relatively immature field such as Information Systems. Many of the benefits, to the members and the wider community, are only fully realised when a professional body is well established and is able to exert real influence within its field of activity.

For me, the most important issue in all of this is whether we see a need for a professional body like the BCS in the IS field? Only when that question has been answered is it possible to make a decision on membership based on the full range of benefits, including those in the medium and longer term. My own view – not altogether surprisingly –

is that there is a very clear need, and a vitally important role, for the Society. More significantly, there is now, I believe, a much wider, and growing recognition of the need for an independent body to set standards and to monitor professional competence, conduct and practice in the area of information systems. Two companies, Logica and General Accident, announced recently that all staff will be required to obtain professional qualifications and many others, including the larger companies like IBM, ICL and Rank Xerox are giving staff very positive encouragement to qualify. There are, of course, those who still argue that professional qualifications are unnecessary or even undesirable in the IS field. The industry has, they claim, done perfectly well up to this point without imposing unnecessary academic, training and other restrictions and it can continue to do so for the future. I have no doubt that there were those who mounted similar arguments when other areas of activity were professionalised in the past – the barbers in the City of London perhaps, when their right to practice surgery was withdrawn in the 16th Century. Unfortunately the facts do not support the argument. The truth is that all is not well in the information systems field and that much of current practice and performance falls short of what could reasonably be regarded as 'professional'. We are all familiar with the well publicised failures over the past few years, but there evidence to suggest that these represent the tip of a much larger iceberg of systems which are defective in some respect.

The September 1994 edition of the journal Scientific American reported, in an article headed 'Software's Chronic Crisis' some fairly depressing statistics, suggesting that one quarter of all large scale software development projects are cancelled, that the average software project overshoots its schedule by half and that some three quarters of all large systems are operating failures, in that they do not function as intended or are not used at all. The same article went on to argue that the main reason for these failures is that much of the activity within the IS field is based on craft practice rather than on established and accepted software engineering principles.

Some would argue that this represents an unfair and overly pessimistic picture of current Information Systems practice, but that would be to miss the point. The essential fact is the ability of the industry to produce systems which meet real requirements, on time and to budget, is on average lower than we would accept in many other areas and our ability to accommodate that lack of quality is diminishing rapidly as we become ever more dependent upon technology and as systems become more complex. If we are to produce the information systems which we shall need for the future, there is an urgent need to build a solid foundation of good practice and to improve the expertise and competence of those involved at all stages of the process.

It is against this background that I see professionalisation as being both urgent and inevitable. I would not claim, of course that the BCS has all the answers to current problems. But I do believe that a chartered professional body, like the BCS, represents the best mechanism yet devised for ensuring that practice within a particular field is built on sound principles and that practitioners are both competent and accountable. Equally important, such bodies also provide a basis for those involved in the profession to play a part in defining, maintaining and monitoring good practice, and in influencing Government, Industry and Academia.

By now you may have concluded that this is aimed entirely at those who fit the Information Systems Engineering definition which is the basis for professional membership of the Society. If so, let me make clear that I see it as essential that the Society attracts membership, and active participation, from all groups with an interest in improving the quality of information systems, including the other professional disciplines involved in the process, those with management responsibility and the users of IS systems and services. Only on the basis of that wider representation and input can we hope to be able to define, maintain and implement practices which will secure systems which are truly fit for purpose.

It is fair to say that the Society, up to this point, not been well equipped to represent this wider community. The Affiliate grade has been available but does not distinguish adequately between the hobbyist and those with a serious professional involvement. However, the new Companion grade will, if approved by the Privy Council, go a long way towards rectifying that deficiency. Companion, which will carry with it the right to use the post nominal letters CompBCS, is intended for those who have a significant involvement in the IS field but are professionally qualified in a discipline other than Information Systems Engineering. It is not yet clear when we are likely to receive a response from the Privy Council but I expect it to be before the end of the year. At that point I hope it will be possible to recruit many of those who have an involvement with BCS, particularly those in the Specialist Groups who have not yet taken up membership.

The opportunity – or perhaps the responsibility – to support and to play a part in the development of the profession represents, I believe, an important reason for joining the Society. However, just in case all this sounds too much like jam tomorrow, let me make the point that the current package of benefits and services does now contain real value. Recent additions to the package, including the new IText publication, the BCSNet service and the publication of the first BCS yearbook since 1990, are adding significantly to that value and the aim will be to add further services as membership, and subscription income, increases.

Anyone interested in BCS membership, including the proposed Companion grade should write to me at BCS HQ or e-mail to cthompson@bcs.org.uk. Comments on any of the issues raised in this article, by the same route, are equally welcome.

BCSNet

Andrew Wilkes

BCS - Head of Technical Services

BCSNet, a combined information provision and Internet access service, was launched on 1 May this year, and publicised via a free cover disc supplied with the April *Computer Bulletin*. As this disc went mainly to BCS Members, it is likely that some SG members will not have received it. Copies are available for bona fide Specialist Group members, from the BCSNet administrator at BCS Headquarters (contact details below).

While the ability both to subscribe to the Internet access service, and to use the free 80 hour Internet demonstration are restricted to BCS Members (of any grade), the disc does carry a World Wide Web (WWW) browser which allows anyone to look at a "snapshot" of the BCS WWW pages – effectively giving those new to the WWW an idea of its "hypertext " nature. In addition, special offers are available – to SG members only – for the waiving of the access registration fees (details from BCSNet administrator) on joining the Society as an Affiliate Member.

But back to BCSNet. This initiative comprises two separate but related parts.

Information provision

The Society has in place an editorial station for the design, development and implementation of electronically held information on all aspects of the Society and related issues – whether general information on Professional Development, publications, codes of conduct, etc., or specific details of Branches and SGs. A dedicated server is being managed for this purpose, and the information will be held largely in WWW form. Basic information is already in place and will be updated and added to on a regular basis. Those with Internet access can look at the "live" version by pointing their WWW browser at the "Uniform Resource Locator" (URL): http://www.bcs.org.uk/

This information is in the public domain – you don't have to be a subscriber to the BCSNet access service. Any full Internet access service will do.

Internet Access

The second strand is designed to promote the "Wired Society", encouraging as many Members as possible to take up electronic access to the Internet. Through a special arrangement with providers "CityScape Internet Services Ltd", the Society offers two distinct access methods.

BCSNet.lite – Unique, we believe, is an offer to all BCS Members, of an email address for life. The BCSNet.lite service is available for a one-off registration fee of £10+VAT, and provides an email addressfor life of the form <amember@bcs.org.uk>

Even those with Internet mail addresses can find this useful, as it also provides free, automatic mail forwarding, enabling the user to use that address no matter which provider actually supplies the connection. In particular, students, contractors, people moving jobs or access providers, etc., need only have the one BCS address. On instructing the server to forward mail to any new address, all mail will be automatically forwarded from <amember@bcs.org.uk> to the specified address.

In addition, this service offers: access to a text only version (but complete with hyperlinks) of the BCS WWW pages; the ability to send and receive Internet email and "Mime" attachments via the server. Aside from the initial registration and the cost of the phone calls (only dial-up to Cambridge) there are no ongoing charges, and the service is available as long as the user is a BCS Member.

BCSNetlite will run on most computers capable of running simple VT220 emulation. While faster modems are preferable, cheaper 2,400 baud modems are adequate for Net.lite.

BCSNet.gold – A specially customised package providing full Internet access, available for a one off registration fee of £25 + VAT and monthly payments of £12.95 + VAT. This provides connection software, Mime compliant email, a news reader and a fully functioned WWW browser. All Gold users are also provided with 0.5M of space on the BCS server for their own WWW pages or file storage area and can use the automatic mail forwarding service.

All this software is fully licensed, (with no shareware fees to pay) and fully supported. In addition, the quality of the support and Network infrastructure is of high quality. At present, there are 6 Points of Presence offering local dial-up charges to many Members. No announcements can yet be made, but it is expected that this number will be expanded considerably in the near future.

BCSNet.gold is available for PCs running Windows 3.1 (a 386 processor or greater, 4 M of Ram and 4 M of disc space are required) and Macs running System 7. Only modems capable of running at 9,600 baud or greater are supported.

Full details of both these services, and of the special deal for SG members for Affiliate Membership of BCS are available from Paul Jones, BCSNet Administrator on 01793 417426 (email: netadmin@bcs.org.uk)

Each SG and Branch is being provided with 3 free registrations for

the .lite service for the use of committee members. Groups also have the opportunity to have their own WWW pages on the server (an initial version of those for CASG can be found in the SG section on the BCS pages). Where possible, they will be encouraged to build and maintain their own pages, linking them into the BCS central pages – eg., by the Group purchasing a Gold account and using the free storage area – but, particularly in the early stages, help with the design and maintenance will be provided through the BCS editorial workstation.

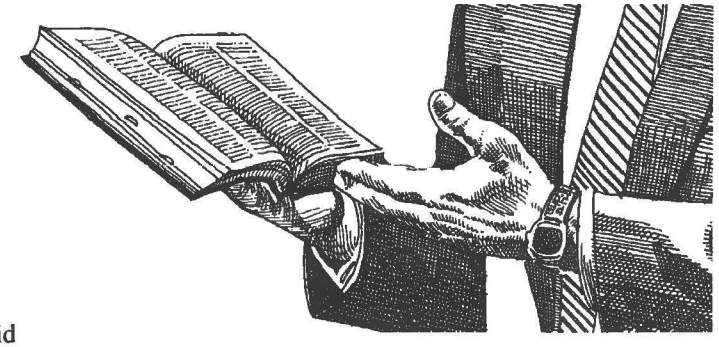
Finally, we are putting a mechanism in place for the development of automatic "list servers" that will enable, eg., a CASG email list to be set up to which members can "subscribe "and "unsubscribe" – thereby receiving copies of all email sent to the CASG list. Similarly, a subscriber with full Internet access will be able to set up a Usenet News Group, either moderated or unmoderated, or the discussion of matters of interest.

We expect more and more of the Society's business to be carried out electronically, and want to encourage as many members as possible to put themselves in the position to participate in this "democratisation". If you have access to the WWW, please feel free to comment on the pages and send your suggestions by emailing the contacts shown there. We look forward to receiving your thoughts.

The Paperless Office

Heard on Radio 4: "The paperless office is about as likely as the paperless toilet"

Book Review



TITLE: Computer Audit and Control Handbook

AUTHOR: Ian Douglas (with additional material from David Bentley, Steve Hinde & Alan Oliphant)

PUBLISHER: Butterworth Heinermann

ISBN: 0 7506 1926 0

PRICE: £25.00

PAGES: 238

REVIEWED BY: JOHN MITCHELL

I first saw this book on the bookstand at this year's COMPACS. For those of you new to computer audit, COMPACS is the Institute of Internal Auditors' annual conference on computer audit and control and it is therefore, no coincidence that this book has been published in conjunction with the IIA. There is a further causal link. The author is a regular day chairman at COMPACS and his own material in this book is supplemented with contributions from three other major players in the field, including two past presidents of the Institute. This is a practitioners book for practitioners and you cannot get more practical than these four. They have been in the business for a long time and the end result is a very useful introduction to the main areas of computer audit.

The author makes this latter point in the preface where he states that 'the objective of this book is to provide an introduction to computer audit for new recruits to computer audit, and for financial auditors who wish to increase their knowledge of computer auditing'. Do not expect to find therefore, esoteric arguments regarding exposure windows in real-time systems, nor detailed discussions on risk analysis techniques. What you will find is good solid common sense, an absence of check lists (praise be) and a fairly easy read. There are also some surprises in a book aimed at this level: a useful appendix dealing with RACF, a good explanation of MVS and an excellent chapter on databases.

Now each chapter could be expanded to form a book in its own right, but the aim of this book is to provide an introduction and it does that very well. It is as up to date as any textbook can be in that it deals with CASE techniques, OOPs and RAD. If you do not know what these are, then you should go out and buy this book, regardless of your position and experience.

So would I give this to my new junior computer auditor? The answer is yes.

Abstract

Companies with sensitive or critical systems face two main problems: no computer security measure can ever be 100% effective, and highly secure systems are highly expensive. This paper poses the benefits of the holistic approach, whereby an integrated, 'across-the-board' security policy is implemented, rather than specific measures to counter specific perceived threats. The holistic approach is shown to benefit security by providing a high level of security for a relatively low cost. A security evaluation model, the 'Five Shields' model, is created to show up vulnerabilities of security policies and assess the strength of protection provided.

Secure Systems in the Finance Industry – The Benefits of a Holistic Security Policy

(Part 2 of 3)

G.S. Leeming and A.M.C. Leeming

3. Complicating Factors

Damage to Reputation

When any company admits that it has suffered a significant security breach, investor confidence in that company is adversely affected. This problem is especially acute in the airline industry, where customers place a great deal of trust in safety, and the financial sector, whose customers can be regarded as investors, as they entrust their money into the care of the institution. Such a crisis of confidence can have a serious effect on the profits of any financial institution.

Deposit-taking institutions can broadly be split into two types: those that offer a guaranteed low level of income, such as high street banks; and those that offer a high level of income in return for accepting risk. If an institution of the first type suffers a publicised security breach, investors see an element of risk in their investment, which negates the reason for accepting a low income. Risk-takers investing in the second type of institution accept risk in the financial markets, and expect a rate of return that will repay them for this risk. When an unrelated risk is introduced, investors may take their business to an institution that is perceived to offer only market-related risk.

As a result of this, there is an industry-wide culture of not revealing security breaches. This is understandable when the damage to reputation can cost an institution far more than the original breach. Even when the perpetrator of a breach is discovered, prosecutions are often avoided in order to avoid publicising the breach (NCC Survey, 1991).

However, computer security in the financial sector can and should be used as a positive differentiator between companies. If it is true that an image of insecurity will damage an institution's reputation, then carefully publicising an image of computer security should enhance that reputation. There is a great deal of public relations value to be gained by advertising an organisation's culture of security, and this can be easily achieved without making details of security measures public.

The National & Provincial Building Society are initiating this trend of service differentiation through security, by producing credit and debit cards containing a photograph of the authorised user. In doing so they are admitting that there is a risk of fraud in the use of credit cards, but creating an impression that the risk is lower with N&P cards than with those of their competitors. Whether photographs on credit cards actually do reduce fraud is a matter for debate, but N&P are creating the right image.

If Chelsea Ltd. were to improve their security to above average for the stockbroking business, the resulting advertising potential would give them an advantage over their many direct competitors. Currently, there are so many small stockbrokers giving such a similar service that it is difficult to differentiate between companies. Security could answer that problem.

The Difficulties of Prosecution

The Computer Misuse Act of 1990 has been widely condemned as an ineffective and insufficient deterrent (Computing, 25/03/93). The Judiciary and Police hierarchy have been branded as failing to comprehend the scale of the problem (Computing, 25/03/93). The Computer Crimes division of the Fraud Squad does not have the resources to effectively combat Computer Crime: 85% of detectives in the Fraud Squad have had no computer training at all (*Reportage*, BBC2, 01/06/93).

But the problems that the Police face are not just resourcing problems: they also have to content with public attitudes towards Computer Crimes and with the often highly complex nature of the offence itself.

The NCC Survey of 1991 showed that of those respondents with disciplinary measures in place, only 6.6% followed a policy of reporting all incidents to the Police as a matter of course. However, in Finance and Business Services, 9.9% of respondents followed such a policy.

Information Systems are usually highly complicated objects, and they are not easily understood without a solid grounding in the fundamentals and jargon of computing. This makes computer crimes difficult to prosecute in the courts, as it falls to the prosecution to explain all the issues involved to a possibly computer-illiterate jury. To be able to understand the nature of an IT-based fraud against Chelsea by their software suppliers, committed using CHAPS, the court would have to possess at least a basic knowledge of data communications, IT security, UNIX system administration, the finance industry and EFT systems.

Norman (1983) estimates that only 10% of computer crimes lead to prosecution, and that only 50% of these prosecutions are successful.

Limiting Speed of Operations

The Finance industry relies to a high degree upon speed of operations. Chelsea's operations in the stock market are a useful example: stockbroking companies have been known to pay large sums for computer systems that will shave just two seconds off the time required to receive information and carry out a transaction. In such an environment, it is essential that computer security can be effected transparently. If security procedures interfere with the normal operations of a system, there is a risk not only that it will affect the organisation's ability to function at maximum efficiency, but also that users will attempt to by-pass security, thereby rendering it invalid.

When a new system is being designed, the *time-criticality of operation* of each of its functions should be investigated, and security measures tailored to avoid damaging this.

Measuring Return on Investment

It is the nature of competitive business that no investment is undertaken unless the benefits outweigh the costs. A financial management view may well look for a suitable return on investment (ROI) and a potential profit margin. As the value placed on security cannot always be expressed in these positive monetary terms, an ROI approach is often inappropriate.

One method of forcing the problem to fit the solution is to use a monetary risk assessment method (see 4.1.). This provides the estimated opportunity cost of not having security, and can therefore be used as the ROI.

It is clear that there has to be a price paid for security, and it is important that this price be balanced against the potential benefits to any organisation. But it is important to realise that this cost is not just measured in monetary terms, but that there may also be a price to pay in effort, time, productivity, and efficiency.

For example, if Chelsea Ltd. were to install a link to SAEF[8], the London Stock Exchange's automated trading system, it would be advisable to protect this link. SAEF allows users to buy and sell shares directly from a terminal, and therefore an abuse of this system could have serious repercussions for Chelsea. If a secure version of SAEF could be purchased for a relatively low price, it might be seen to be a good investment. However, if this secure version were to slow down the human-computer link, for example by requesting passwords to verify authorisation of deals struck, it would have a severe effect on its users' productivity, and so it might cost Chelsea more to install the secure version than to accept the risk of fraud.

4. System Security Controls

A wide variety of security countermeasures are available to any interested party. This section provides a brief overview of the main types of countermeasure, split into five categories: quantification measures, aimed at improving information about the problem; personnel and procedural measures, designed to reduce the opportunity for computer crime; deterrence measures, intended to deter people from attempting to breach security; defence mechanisms, designed to make security breaches harder to commit; and finally minimisation measures, intended to reduce the possible consequences of any security breach.

Too many organisations rely on measures from just one, or maybe two of these categories. However, no single type of measure can completely protect a system, and cannot operate at full efficiency without the support of other measures. For example, there would be little point in Chelsea Ltd. introducing a security policy setting out every employee's duties, proscribed activities and their possible consequences unless it was supported by increased systems security. Under the present set-up, such a policy would not be taken seriously by the staff, and so the effect would be lost. Similarly, the introduction of a new, improved access control system would not have any significant impact on the company's security unless supported by a security policy that changes the organisational culture of sharing passwords.

A well balanced secure system should include preventative measures from each category, along with detective measures such as accountability and system audits. The synergistic effect thus gained, coupled with a system prepared for all possibilities, has a dramatic effect on any system's security. The five shields model described in section 5 sets out a method of ensuring that a security policy is comprehensive and sufficient to counter the existing threats.

[8] Stock Exchange Automated Execution Facility.

Quantification Measures

The first step in combating any problem is attempting to understand the situation. In the case of computer security, this means attempting to evaluate and/or quantify the existing threats to the system, and analysing the ability of any preventative measures to prevent breaches. Quantification measures can be viewed as the preliminary research necessary to tackle the problem.

Security Evaluation

Security evaluation can be performed on any IT system of item of hardware or software. It analyses the level of trust that can be placed in the security of the system or product, and evaluates the degree of protection provided. There are three main benefits arising from having a system evaluated. Firstly, it analyses the likelihood of software or hardware failures leading to denial of service; secondly, it provides assurance that the secure components of the system are capable of withstanding direct 'attack'; and thirdly, it supports 'due diligence' arguments in case of audit or insurance problems.

The ITSEC[9] scheme is currently the European standard scheme for security evaluation. It is run by the Dept. of Trade and Industry and CESG[10] at GCHQ Cheltenham. By 1999 it will have been superseded by the Common Criteria, a world-wide standard. The ITSEC scheme supports the holistic approach to security. As with most security evaluation schemes, system security is measured across a number of key areas, and overall security expressed as a function of these areas. Other schemes, such as the TCSEC scheme in the USA, or the CTCPEC scheme in Canada, use a function similar to taking the mean: i.e. if a system has strong security in one area, and weak security in another, it will be evaluated as having medium security overall. But the ITSEC scheme takes the minimum level: for a system to be evaluated as having 'level X' security overall, it must be evaluated to level X in every area. This is regarded by the security community as one of ITSEC's strong points (alt.security, 1993/1994).

Risk Assessment

Commercial computer security is essentially an exercise in risk management, and as such needs the support of risk assessment. Risk assessment provides a formal methodology to identify and measure all risks, vulnerabilities and threats applying to a computer system.

Its main advantages to a manager interested in security are:

- it specifies appropriate and sufficient counter-measures (risk management and risk reduction)
- its results can be used to quantify the possible costs arising from security breaches and thereby justify expenditure on security.

However formal its methods, a risk assessment does rely to some extent upon personal judgement and estimates of the likelihood of threats materialising. Therefore its results can only be an estimate, and should not be taken as exact. Risk Analysis and Management is an art, rather than a science. As with all estimating methods, however, its results can be refined by improving the quality of the information used, and by gradual improvement based on experience.

Risk Analysis supports every other form of countermeasure. By providing detailed information on the level of risk involved with each threat, it allows the security designer to tailor the level of protection provided by each countermeasure more exactly to the existing threat.

CCTA, the Government Centre for Information Systems, has produced a computer-based package called CRAMM, the CCTA Risk Analysis and Management Method.

Personnel and Procedural Measures

The biggest problems in securing any system are caused by the people who use it (Burch & Grudnitski, 1989). Almost all security measures rely on the co-operation and support of the users, and so without that support they cannot properly fulfil their functions. Businesses can no longer rely on the ethics of their staff to prevent them from breaching security, and should therefore take appropriate personnel measures.

Rotation of Personnel

The longer an employee stays in one position, the better he or she will become acquainted with system loopholes. Personnel in security-critical positions should be rotated regularly to other posts to avoid this. This policy is often adopted for other reasons: personnel left in one position for a long period of time tend to suffer a lack of motivation, and develop a short-sighted approach to their work.

However, there is a fine line to be drawn between rotating personnel so slowly that they become a potential security problem, and rotating them so fast that they don't have time to learn their jobs. This fine line will be different for each person and for each post.

Warning Signs

Bologna estimated that 20% of people would steal under the right circumstances (q.v. 2.5.). Ideal personnel & procedural measures would screen out this 20% from potential recruits, remove motivation from any that might already be a part of the company or pass the recruiting screens, and detect 'criminal' behaviour before any crime can be committed.

---

[9] I.T. Security Evaluation Criteria

[10] Communications and Electronic Security Group.

A number of classic warning signs exist that often point towards potential or existing criminal behaviour. Although not an exhaustive list, the most common of these are:

- Abnormal working hours.
- Personal stress.
- 'High Living', or spending patterns out of proportion to salary.
- Sudden interest in company information or practices not associated with normal work.

Need to Know

The exposure of a company's information can be limited by restricting access to those of its employees who have a need-to know. A need to know can be defined as needing access in order to adequately perform one's duties. This is simply adapting an existing practice to computer security. Many companies keep details of their operations secret from their employees. This should not be taken to mean that the company does not trust any of these employees, but just as a risk limitation measure.

When extended to computer security, a need to know policy can cause problems in classification of data. In order to give an employee access to certain data only, that data must be given some form of label. It is not practicable in any but the smallest of companies to change access privileges for every person for every document. Instead, data is labelled, and each user given access to certain labels only.

Having a need-to-know policy active supports the use of access controls (q.v.). Personnel can see the reason for the policy, and are therefore more likely to accept and abide by the controls. However, as with all policies, need to know must be upheld at all levels. If their manager does not abide by the policy, staff will not either.

Responsibility Limitations

Where practicable, critical tasks such as the transfer of large sums of money should not be the sole responsibility of any one person. There are three ways of achieving this: the two person rule; splitting a task into distinct parts; or requiring separate authorisation. The two person rule, when applied to a function, requires two different people to be logged in simultaneously and separately perform the function in order to gain authorisation. Similarly, a task can be split into two or more parts, and system privileges can then be used to ensure that one person can only perform one of these parts. Finally, authorisation from senior personnel, who may be considered 'above reproach' and paid appropriately, can be demanded.

These measures guard against 'lone-wolf' fraud, but can be bypassed by conspiracy. They each have their drawbacks, in that they slow down a company's operations, and can be bypassed without a great deal of difficulty. It is also difficult to determine in advance what might constitute a critical task.

In Chelsea's case, responsibility limitations are only useful on the EFT system, where they are already in place. In the dealing room, almost every deal could be a critical task. Requiring senior authorisation or responsibility sharing on every deal would slow down dealing operations to such an extent as to make them impractical. In practice, dealer limits can be imposed, requiring a dealer to obtain authorisation only for transactions that exceed their limit, and transactions can be reviewed regularly by a senior dealer.

Deterrence Measures

Deterrence measures are aimed at preventing breaches before they occur. In this they should attempt to remove the motivation behind crime, and reduce opportunities to breach security.

Security Policy Document

A Security Policy Document should be an integral part of any secure installation. Too often, employees are unaware of their duties and obligations towards security, and can compromise security without realising. Each employee with access to the IT systems should know what their responsibilities are, what they should not do, and the penalties of breaching security. A formal security policy document, distributed to each employee, is a good method of ensuring that this information is taken in.

De Maio (1992) asserts that to ensure maximum effectiveness, a security policy document should:

- Be positive, not negative. Nobody enjoys being hedged in with a long list of 'Thou shalt not's.
- Be visible to all staff.
- Be readily understandable. The policy will apply to employees of widely differing levels of computer knowledge, and therefore should avoid jargon and acronyms in favour of plain English.
- Contain realistic and enforceable penalties. It is no use threatening automatic dismissal for all offences if senior management or unions will overrule this. For example, threatening that security breaches will be punished by a dawn firing squad, even in jest, encourages employees to treat the whole security issue as a joke.
- Be supportive. The policy is ultimately aimed at helping employees carry out their job safely and with appropriate integrity.
- Be feasible. Can the average user achieve what the policy asks? For example, if a user has access to ten different systems with ten different passwords, all changed at regular intervals, it is not feasible to

ask that user not to keep a record of his passwords. Instead, the number of passwords required should be reduced, or a method found of recording the passwords that is comprehensible only to that user.

- Cover information in all forms, not just computer-based. For example, Chelsea would gain very little from securing their commissions database if their employees regularly discuss commissions levels in the pub at lunch time.

A well-formulated and visible document will directly change the two main motivations for crime discussed in section 2.5. Such a policy will ensure a culture of security, and employees will not be so predisposed to believe that they can easily get away with security breaches. The view that 'stealing a little won't hurt the company' may still exist, but, with enforceable penalties for breaches, potential fraudsters will realise that stealing a little might hurt them. The culture of security supports every other security countermeasure. As Burch and Grudnitski (1989) point out, the biggest vulnerability of any countermeasure is the people who use it. If those users accept, understand and support the culture of security, then the countermeasures can work more effectively.

Audits

System audits are also useful for discovering previously unnoticed breaches. Certain forms of fraud, rogue programs and hacker attacks rely on subtle modifications to system attributes. A well-known form of electronic fraud is the 'Salami' technique, whereby an EFT system is modified to slice off very small amounts from a large number of transactions and redirect them to a separate account. 'Trojan Horses' act this way: a Trojan horse is a rogue program masquerading as a part of the system software. For example, a typical Trojan horse might impersonate the log-in process: where the normal log-in process would ask for user name and password, and if given correctly, allow the user into the system, a Trojan horse would ask for user name and password, save these where they can be retrieved by an unauthorised third party, and then allow the user entry to the system.

System audits can range from simple, automated audits to large scale investigations of the system. Even simple audits will often catch such breaches as described above. One form of automated audit is the 'Checksum' audit, which is a simple and fast method to detect additions or modifications to the system. When the checksum audit is first implemented, it records the size or 'checksum' of each application and/or datafile on the system. On subsequent audits, it re-measures all checksums and compares them against the original findings. Any application or datafile which has been modified will have increased or decreased in size, and so the checksum will be different. This procedure can be personalised to ignore items that are expected to change size during normal operation of the system, such as user datafiles.

A high proportion of the costs involved in a security breach are those of detecting and assessing the damage caused. This is especially true of a hacker attack: a hacker that has attained super-user status could have gone anywhere in the system and altered any file or application. This means that every part of the system must be checked in detail, and this can be a very expensive process. Good system audit procedures minimise this cost by providing a record of exactly what has happened to the system.

By restricting the ease of modifying the system, system audit procedures support anti-virus measures (viruses spread by modifying the system), and, as described above, anti-hacker procedures.

Anti-Fraud Measures

Anti-fraud measures are being pioneered in the fight against credit and debit card fraud. Most such measures are based on expert systems or neural networks, and attempt to identify patterns of fraudulent behaviour as they occur. In credit card fraud, examples of such behaviour include:

- Regular purchases at or just below the card's authorised limit.
- Multiple purchases of consumer electronics during a short time, for example buying three televisions in one day.
- Large transactions far from the normal geographical area of use.

Barclays Bank have developed an expert system known as Cardwatch, and claim that it detects on average 40 fraudulent transactions every week.

These measures are currently in their infancy, and so have a limited application outside credit card fraud. However, as these products are developed, they will become useful in detecting more forms of fraud. Current problems include:

- Not all identified patterns actually constitute fraudulent behaviour. Some people actually do buy three televisions in one day.
- Anti-fraud systems need to work on a large number of transactions with established patterns of fraud. This makes them of strictly limited use for smaller-scale problems.
- Designing and implementing such a system is very difficult, and therefore expensive.

Defence Mechanisms

Physical Defences

All physical threats can be guarded against to some degree. The following is a list of the standard forms of defence against the more significant breaches.

Loss of power

Universal Power Supply (UPS) systems are available for any system. These devices detect power failures and replace the interrupted power with battery power for a limited period. This is sufficient to guard against all but the most serious of power failures.

Unexpected Hardware or Software Failure

These are the most difficult to guard against, as by definition they are unexpected. Systems assurance can be carried out, but it requires highly skilled staff and is correspondingly expensive. The best defence is a regular backup procedure and/or a mirrored hard disk to minimise the potential consequences.

Natural Disasters

Protecting against natural disasters does not fall under the responsibility of the IT Security Manager, although standard precautions against fires should be taken in any computer room. Minimising the effects of such a disaster is part of the Manager's responsibility: with a good disaster recovery site (q.v.) and regular backups (q.v.), most organisations can be up and running within hours of any disaster short of widespread destruction. However, contingency planning should be carried out for such an event to ensure that a complicated office move can be effected quickly and effectively.

Physical Access Control

Physical access controls, such as locks on doors, security guards, security badge systems, act against most external threats, by reducing access to the machines, and help to enforce need-to-know policies and logical access control mechanisms. Physical access controls can be used to keep unauthorised users out of the building, and to restrict access of employees within the building to those areas to which they need to have access as part of their work.

Physical Access Controls, surprisingly, have an effect on hacking. Sterling (1992), Hafner and Markoff (1991) and Cornwall (1985) all note the widespread hacker practice of wearing a suit and briefcase, and wandering into office buildings during the lunch-hour, finding an unattended terminal, and sitting down and seeing what's on the system. Physical Access Controls deny this opportunity.

Access Control

Otherwise known as system 'privileges'. Access control allows parts of the system to be made accessible only to certain users. This supports the implementation of a 'need-to-know' policy.

User Identification

The most common form of computer security, user identification, ensures that only authorised users are permitted entry to the system. This is most commonly effected by a 'user name' and password, but biometrics systems[11] are being successfully launched on to the market. Being the most common form of security, it is also the most open to abuse. Password sharing, the use of common passwords such as 'FRED'[12] or 'QWERTY', and the practice of writing down passwords in an accessible place are all widespread practices. User identification supports systems audits: audits list system actions and their system 'owner'. If the user identification procedure is in place, secure and reliable, then audit reports of system owners can be relied upon.

Data Encryption

Advances in mathematical cryptography have ensured that there are easily affordable encryption systems that are not practically possible to decode without the appropriate key. This enables external data communications to be rendered highly secure for minimal cost. If Chelsea were to encrypt their sensitive data on the system, it would ensure that no hacker could obtain access to the information. However, this does not protect the information from a fraudulent employee with access to the key.

Tempesting

All computer systems emit electromagnetic radiation that, with the right equipment, can be readily received and decoded from a distance. Such equipment is legal and relatively easy to obtain. Thus a hacker with the appropriate skills could sit outside Chelsea's offices and legally 'read off' any data displayed on any screen within the building. Tempested terminals are shielded to prevent such emanations and eliminate this problem. However, such eavesdropping is not a common practice, and usually tempesting is only carried out to protect extremely valuable or sensitive information.

Dial-back

A simple anti-hacking measure for systems that need to support external connections from specified, authorised locations only. Instead of dialling straight into the computer via a modem, the user connects to the dial-back mechanism, and tells the mechanism the telephone number he is using. The mechanism drops the connection, checks the number against an authorised list, and, if the number appears on the list, dials back the user, and places the connection from the other end. This also has the fortunate side-effect of ensuring that telephone billing is centralised, making accounting practices somewhat easier.

Virus Disinfection

Viruses can be protected against with relative ease. A wide variety of 'vaccination' and 'disinfection' software exists on the market; they are updated regularly

---

[11] e.g. voice recognition or fingerprint recognition

[12] The four letters of 'FRED' are adjacent on a standard keyboard.

to keep up with the latest advances in virus technology. If installed on all processing sections of an IT system, these can provide a very high level of low cost protection. Two simple operating procedures can also drastically reduce the chance of infection: firstly, to ban unauthorised software, such as games and shareware, on company machines; and secondly, provide stand-alone PCs with no data links and no functionality except virus detection and disinfection to act as 'gatekeeper' PCs. If all new disks are checked on these machines before use on the system, viruses can be detected and removed before they come into contact with sensitive machines. It is worth noting that there have been very few reported attacks by mainframe viruses.

Minimisation Measures

Largely self-explanatory, these measures attempt to minimise the damage arising from security breaches.

Backups

Backups are a standard part of almost every IT installation, and a well-managed daily procedure, for example, will limit the loss of data from a serious failure to only one day's work. If at all possible, two copies of all backups should be kept: one copy on site for rapid restoration, and one copy off site in case of a large scale disaster such as a fire or flood.

Disaster Recovery Sites

A disaster recovery site is a separate installation with identical systems and hardware and backup copies of system data. It allows an organisation to continue operating its IT systems with minimum disruption in the event of a large-scale failure of the original system. Disaster recovery services are now offered by a variety of companies, especially in the finance sector.

Disaster recovery sites come in four flavours: 'Cold', 'Warm', 'Hot' and 'Flying Start'. A hot site is one which has identical systems, is constantly available for use, and contains regular backups of system data. A flying start site is a hot site with mirrored storage media: all data or applications saved to the live site are simultaneously saved to the flying start site. A cold site consists of available space to recreate the system, whether owned or part-leased, and an agreement with the system suppliers to supply new hardware and software as fast as possible. Cold sites are of limited use, as they can take weeks to bring up to operational capability, and hot sites are extremely expensive to maintain. The standard compromise is a warm site, especially in the finance sector. A warm site is a disaster recovery site that has 'hot' characteristics and 'cold' characteristics. An example of this, and most appropriate for Chelsea Ltd., is the service operated by Dealing Room Disaster Recovery Ltd. of London. The company own premises that have all the appropriate hardware to operate as a dealing room. It keeps copies of appropriate software and data on site for all its clients, and in case of a disaster these clients can use the company's facilities with minimal delay: usually only a matter of a couple of hours. This gives its clients almost all the advantages of a hot site, but spreads the cost. The major drawback of this is that the company does not have sufficient facilities to accommodate all of its clients simultaneously. In case of a major disaster affecting a number of its clients, such as the IRA City bombs, each client would have access to a strictly limited service.

Insurance

Insurance is a business necessity, and most if not all companies have insurance. However, not all insurance policies cover losses caused by computer security breaches of all kinds, and any policy should be thoroughly checked against possible threats. Financial institutions can insure against third party computer crime with Lloyd's of London (Investors Chronicle, 26/05/89). Business insurance policies also require due diligence on the part of their owners in guarding against threats. The due diligence argument can usually be supported by deterrence and quantification measures such as risk assessment, security evaluation and security audits.

To be continued in the next issue of CASG Journal

The Authors –

Geoffrey Leeming *developed an interest in IT Security in Finance as part of his studies at Kingston University Business School. He is currently working in the Computer Audit and Security Group at KPMG and studying part-time for an MSc in Information Security at Royal Holloway College University of London,*

Anne Leeming *is Director of the MBA programme, IT and Management, at City University Business School. Her research is in the impact of IT on organisations and in the way they manage with IT.*

Minutes of the Annual General Meeting held at the Royal Institute of Public Health and Hygiene on 10 May, 1995.

Held in the presence of 18 members (28 including late arrivals) of the Group including the Chairman and the Secretary. Apologies were received from the Treasurer.

1. Approval of the minutes of the 1994 AGM

The minutes of the 1994 AGM held on 11 May, 1994 were approved as a correct record of the meeting.

2. Chairman's Report

Dr J.A. Mitchell presented his report for 1994/95 and highlighted the following:

- It was Dr Mitchell's seventh year as Chairman and he is retiring on this occasion. He attributed the Group's success during his chairmanship to the hard work and attention to detail by the members of the management committee and he thanked them for it. He was pleased to have established a good Journal which is valued by the members, especially those that are unable to attend our meetings. Discussion groups started over the last couple of years have also been well received.

- Nigel Smith is away in the USA and is standing down as the Treasurer. Rob Melville is standing down as the Journal Editor and John Bevan is vacating the Member Services position. He thanked them all for their contributions.

- The membership numbers have dropped a little for individual membership but there has been a slight rise in the corporate membership. He observed that as the control of computer systems is so important to today's business, management – including finance managers, should show increasing interest in the activities of our group. Internal auditors were well represented but there were not many external auditors.

- The chairman summarised the meetings held during the year, they covered topics relevant to all auditors. This year the annual conference was cancelled and the Discussion Group meeting scheduled in its place was not successful either.

- Members discounts on training courses and magazine subscriptions were very good value.

- BCS are now over their cash crisis and are now unlikely to call on our funds!

- We have held joint meetings with the ISACA, IIA, ICAEW and we are developing good relations with these bodies.

- He gave the management committee a vote of thanks on behalf of the members present.

Full details of his report will be published in the journal.

3. Treasurer's Report

In the absence of the Treasurer the Chairman presented the draft unaudited Income and Expenditure Account for the year ended 30 April 1995. He highlighted the following:

- our recurring expenditure were not covered by our income, the operational deficit being over some £600;

- the discussion groups made a surplus of over £400;

- last year's conference made a surplus of over £600.

There were no questions raised from the floor regarding the Treasurer's report and the accounts for 1994/95 were accepted by the meeting on behalf of the membership and approved for forwarding to the British Computer Society, subject to completion of the audit.

4. Election of Officers and the Committee

Dr John Mitchell retired as Chairman of the Group and was duly replaced by Alison Webb as there were no other nominations. Raghu Iyer was re-elected as the Secretary and Bill Barton was elected the Treasurer. Dr Mitchell thanked Tony Locke for acting as the Honorary Auditor and he was now replaced by Chris Wright who had offered to undertake this role. All officers were elected unopposed.

The new Chairman Alison Webb took over the Chair at this point. On behalf of the committee and the membership she thanked John for the inspiration, leadership and ideas that helped the committee in going forward over the last seven years, and also for his

dedication and hard work. She noted that Steve Pooley and Jacqui Race were retiring from the Committee and that the remaining Committee members had all indicated there willingness to continue in office. She also thanked John Mitchell for staying on the committee to help as Journal Editor. She asked members present who wished to join the committee to either come forward or speak to her later or drop her a line. She thanked Steve and Jacqui for their support in the past and wished them well for the future. There was one member who volunteered after the meeting to join the committee and was duly accepted to help with organising the Technical Briefings.

The meeting approved the election of the officers, Hon. Auditor and Committee members as noted above.

The committee elected for 1995/96 was therefore as follows:

Officers

Chairman	Alison Webb	Consultant
Secretary	Raghu Iyer	KPMG
Treasurer	Bill Barton	Consultant

Members

Membership Secretary	Jenny Broadbent	
	Cambridgeshire County Council	
Technical Briefings	Paul Howitt	
	Tesco Stores Limited	
	John Bevan	Consultant
	Geoff Wilson	Consultant
Journal Editor	John Mitchell	
	Little Heath Services	

5. The proposed 1994/95 Members' Meeting Programme

Alison Webb said that in view of the poor attendance at the monthly members' meetings and the considerable effort it requires from the organisers we should try some thing different this year. She suggested holding three whole day Technical Briefings covering topics of current interest and with high profile speakers and chair persons. These meetings would be held at a prestigious venue and will be well publicised. She said that Paul Howitt had already arranged most of the detail but full details of the programme will be published in the Summer issue of the Journal.

6. The Journal

Alison appealed to members to submit articles for the Journal and stressed that it was a good way of getting known among the computer audit fraternity.

7. Projects

She informed the meeting of two projects which CASG will be undertaking in the coming year. The first one the updating of the BCS Industry Structure Model and the second was a research project to establish the extent of computer audit activity in the UK. The latter is currently in the proposal stage. Further details of both project will be published in later issues of the Journal.

There being no other business the 1995 AGM of the British Computer Society CASG was closed.

Lotus Bugged

A Freudian slip or simply a slip of the tongue. With software companies you can never be too sure. So what should we make of Lotus's Neil Hudspeth's response to a question on whether or not Lotus maintenance subscribers get priority access to upgrades and bug fixes. "No. It doesn't matter whether a customer is paying for maintenance or not, we'll ship them the latest bugs as soon as possible." We'll give you the benefit of the doubt on that one Neil.

. . . from PC Week

CASG CHAIRMAN'S ANNUAL REPORT 1994/95

For the last seven years I have had the honour to address you as chairman of this group. During that time I have seen membership both expand and contract, the creation of our quarterly journal and the inauguration of our discussion groups. Now I have decided to stand down as chairman so this will be my last report in that capacity. I know that my successor will find new ways to make the role of the group even more vital to the future business environment.

Management Committee

Your management committee comprises four elected positions (chairman, secretary, treasurer and auditor), as required by the rules of the BCS, and a number of volunteers. The chairman is required to be a BCS member and it is desirable that the other elected officials, with the exception of the hon. auditor, are also members, although there is some flexibility on this point.

The list below shows the committee for next season. As you notice, each member of the committee has a defined responsibility and where possible there is some "shadowing" of roles to cater for the invariable moves that take place where professional people are concerned.

Elected Officers

Chairman:	Alison Webb	Alison Webb Associates
Secretary:	Ragu Iyer	KPMG
Treasurer:	Bill Barton	
Hon Auditor	Christopher Wright	

Members & Associated Responsibilities

Membership	Jenny Broadbent	Cambs County Council
Meetings	Paul Howitt	Tesco Stores Ltd
	Jim Ewers	Herts County Council
	John Bevan	Independent Consultant
Journal Editor	John Mitchell	LHS – The Business Control Consultancy

Finances

The report from our Treasurer, which is included elsewhere in this Journal, shows that we made a small operating loss last year, but we are still in a healthy financial position.

Membership

Our membership records show that we currently have some 241 members. This represents a drop of 25 members and is disappointing in view of the importance of Information Technology Systems control in all business sectors. An analysis of the numbers shows that the major drop has been in corporate membership.

By type of Membership	1995	1994	1993	1992	1991	1990	1989	1988
Corporate	141	136	224	245	195	140	139	139
Individual BCS	37	37	64	63	57	45	33	35
Individual Non BCS	62	92	100	106	78	61	34	37
Student	1	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	241	265	355	393	390	301	207	211

By Discipline	1995	1994	1993	1992	1991	1990	1989	1988
External Audit	32	34	26	42	48	47	41	38
Internal Audit	180	196	277	309	290	214	130	151
Other	29	35	52	42	52	40	36	22
	241	265	355	393	390	301	207	211

Discussion Groups

It was intended to hold four Discussion Group meetings during the year, but in the event only three were held due to lack of response to the one scheduled to cover the Internet. The subjects covered were:

Developing a Strategy for Computer Audit

Controls in Electronic Payment Systems

Runaway IS Projects

The format is to have four sessions, each of which is addressed by a speaker for about 30 minutes, followed by about an hour's discussion. We limit attendance to keep the meeting small enough to ensure that discussion actually does take place.

Member Meetings

The annual meeting programme was superbly handled by Paul Howitt and Jenny Broadbent. The subjects covered, excluding our four discussion groups, were as follows:

1994	*Subject*
14th September	Computer Security Policies (joint with BCS Computer Specialist Group)
8th November	Client Server Systems
1995	*Subject*
17th January	Business Process Re-engineering

	(Joint Meeting with IIA)
14th March	Unix Security (Joint meeting with ICAEW IT Faculty)
4th April	Annual Debate with EDPAA

The Journal

Under Rob Melville's stewardship, our main communication arm with our membership goes from strength to strength and it has become the envy of other Specialist Groups within the BCS. For those members unable to attend our meetings it provides valuable information at both a practical and theoretical level on computer audit and control matters.

Other Member Service

We continued to negotiate, on your behalf, substantial discounts for attendance at numerous commercial conferences.

An attempt to survey the requirements of our members received such a poor response rate, despite the offering of a prize, that the results were not statistically meaningful.

Annual Conference

Due to the success of our discussion days and the continuing fall in attendance figures we decided to substitute a further discussion day for our usual conference.

External Relations

Our annual joint meeting with the Home Counties District of the Institute of Internal Auditors was its usual success and we also held our third annual debate with the London Chapter of the EDPAA.

Conclusion

The past year has been a year of consolidation on our past successes which has only been achieved due to the hard work of your management committee. I would like to propose a vote of thanks to them on your behalf, but more especially on my behalf, as without their generous help and support the chairman's job would be impossible.

John Mitchell
15th May 1995

BRITISH COMPUTER SOCIETY - COMPUTER AUDIT SPECIALIST GROUP

DRAFT & UNAUDITED INCOME & EXPENDITURE ACCOUNT for Year ended 30th April 1995

				1994/95	1993/94
RECURRING ACTIVITIES				£	£
Income:	Subscriptions			4,910	5,035
	Interest on bank accounts			1,089	808
	Discussion days	—Income	4,160		
		– Expenditure	3,711	449	600
	Sundry income			250	176
	Joint meetings			113	0
	Unclassified			340	0
Expenditure:	Members' meetings			(725)	(1,735)
	Joint meetings			(130)	0
	Programme cards			(870)	(834)
	Letterheaded paper			(259)	0
	Administration			(840)	(1,145)
	Journal	– Expenditure	5,478		
		– Income	529	(4,949)	(3,828)
	Donation				(500)
Recurring activities surplus/(deficit)				**(622)**	**(1,423)**
SPECIAL ACTIVITES					
	Conference	– Income	5,075		
		– Expenditure	4,446	629	(541)
	Book sales			49	433
Special actities surplus/(deficit)				678	(108)
OVERALL SURPLUS/(DEFICIT)				**56**	**(1,531)**
Fund balance at 1.5.94				30,085	
Add 1994/5 surplus				56	
Fund balance at 30.4.95				**30,141**	

CASG GROUP
OBJECTIVES AND CONSTITUTION

1. NAME

The Group shall be called the Computer Audit Specialist Group (CASG) of the British Computer Society (BCS).

2. OBJECTIVES

a) To encourage research into the audit of information systemsand to promote the development of auditing and control techniques to reflect changes in technology, legislation and society.

b) To provide a forum for the development of awareness and competence in information systems audit.

c) To promote the efficient, effective and economical use of audit and control within information systems.

d) To represent the interests of the Computer Audit Specialist Group to other bodies.

e) To be the primary focus for audit and control matters within the BCS.

3. CONSTITUTION

The Computer Audit Specialist Group shall consist of:

a) The Officers, being Chairman, Secretary and Treasurer, all of whom should normally be members of the BCS.

b) Other officers to represent sub-groups or to perform other tasks which may be determined from time to time.

c) Individual fee paying members.

d) Corporate fee paying members, viz Companies, Groups or other organisations wishing to support the purpose of the Computer Audit Specialist Group.

4. ELECTED OFFICERS

a) The officers shall be elected by the Annual General Meeting (AGM) and shall serve from their time of appointment until the end of the AGM following.

b) A vacancy occurring during the term of office may be filled by an appointment by the Management Committee.

c) Other officers may be nominated to fill any other posts created by the Management Committee.

5. MANAGEMENT

a) The affairs of the Group shall be managed (subject to the control of the AGM) by a Management Committee comprising:

1) Elected officers

2) Co-opted officers

3) Elected members

b) Co-Option: the Management Committee may co-op members as required.

c) Meetings: The Management Committee shall meet at least four times in its year of office and frequently enough to properly carry out the business of the Group.

d) Notice: At least 14 days notice of the place, date and time of meeting shall be given to each member of the Management Committee.

e) Quorum: The business of the Management Committee may be transacted by not less then four members.

f) In the absence of the Chairman, the committee shall elect one of its number to take the chair for the meeting.

g) Voting: In determining a question by vote at a Management Meeting a simple majority will be sufficient. The chairman of the meeting shall have a second or casting vote if necessary.

h) Sub-Committees: The Management Committee may appoint at any time sub-committees with appropriate terms of reference, each responsible to the Management Committee and under the Chairmanship of a Management Committee member, to assist in carrying out the business of the Group.

i) Working parties: The Management Committee may set up at any time working parties responsible to the Management Committee which shall appoint a Chairman and provide appropriate terms of reference.

j) Branches: The Management Committee may set up at any time branches responsible to the Management Committee which shall appoint a Branch Chairman and provide appropriate terms of reference.

6. ANNUAL GENERAL MEETING

a) Each year the Group shall hold an AGM not later than May.

b) Notice: The Secretary shall send notice of the date, time and place of the AGM to all members of the Group at least 28 days before the Meeting.

For this purpose a notice printed in the Programme Card of the Group and complying with the above requirements shall be considered sufficient notice.

c) All members of the Group have the right to attend the AGM, for which there shall be no attendance charge.

d) Agenda: The following items shall be included:

1) Minutes of the previous AGM
2) Minutes of any Extraordinary General Meeting held since the previous AGM
3) Chairman's Report
4) Statement of Accounts
5) Proposals for alterations to the Constitution
6) Proposals for alterations to Fees
7) Election of Officers
8) Election of Auditors

e) Nominations: Any member is entitled to nominate a person for any elected office on the Management Committee. Such nominations may be proposed and seconded at the meeting if not previously received by the Secretary.

f) Voting: Every question at an AGM shall be decided by a simple majority of the votes cast. Individual members of the Group each have a single vote. The accredited representative of each corporate member also has a single vote. The chairman shall have a casting vote if necessary.

7. EXTRAORDINARY GENERAL MEETING

a) An Extraordinary General Meeting (EGM) shall be convened on a resolution of the Management Committee or within five weeks of receipt by the Secretary of a requisition signed by no less than twenty members (Corporate members having only a single vote) stating the business to be transacted at the meeting.

b) An EGM shall transact only such business as is specified in the resolutions or requisitions convening it.

8. FINANCE

a) Bank account: In accordance with BCS Guidelines, the Group shall have at least one Account (Account A) at Lloyds Bank, Langham Place Branch, used for normal running expenses. Other accounts at that branch or other places as approved by the Management Committee, may be used for special events or for investment funds.

b) the Group shall follow the BCS Financial Guidelines as issued from time to time.

c) The financial year shall start on 1st May each year.

d) The Treasurer is responsible to the BCS for submitting draft budgets, recording ongoing expenditure and capital expenditure separately for each by 30 November in the preceding year.

e) The Treasurer is responsible for making available to the BCS a revenue statement at the end of every financial year (30th April) in respect of the Group's normal operations and special events, this statement to be included in the BCS annual accounts subject to audit by the BCS auditors.

f) All cheques drawn on the Group's bank accounts must be signed by any two of Chairman, Secretary and Treasurer. In the event of such signatories being unavailable, then the Management Committee may appoint a member of the Committee to act as second signatory, together with one of the nominated signatories.

g) The accounts of the group shall be audited each year by an auditor elected at the AGM.

h) All income and property of the Group from whatever source derived shall be applied solely to the promotion of the objects of the Group.

9. DISSOLUTION

In the event of the winding up or dissolution of the Group any surplus assets remaining after discharge of liabilities shall automatically rest in the BCS.

In the event of an authorised officer of the Group not being available to conduct the transfer of any assets, then an appropriate officer of the BCS shall have the required power.

10. BRITISH COMPUTER SOCIETY

a) The Group shall be governed by the rules of the BCS as these apply to Specialist Groups of the BCS. Where it is considered that a rule of the Group is in conflict with a BCS rule governing Specialist Group activities, the BCS rule shall apply.

b) The Chairman of the Group must be a Fellow, Member or Associate Member of the BCS.

c) Other elected officers of the Group should normally be members of the BCS.

d) The Chairman, or other elected Committee Member of the Group, is ex officio a member of the BCS Technical Board.

e) The Group must advise the Chairman of the Technical Board of the names of any elected officers who are not members of the BCS.

f) All members of the Group's Management Committee shall abide by the Code of Conduct relating to members of the BCS.

g) The Group may use the BCS name to enhance the reputation of their own activities, but must not bring the BCS into disrepute.

h) No member of the Group may speak on behalf of the BCS without proper authority from the BCS.

Problems of the Internet

John Silltow – Security Control and Audit Limited

What is the Internet? It is a loose collection of networks and users throughout the world who are linked electronically. The numbers are large and have been quoted as 75 countries and 30 million users with new members being added at the rate of 1 million a month.

For marketing purposes, the Internet is a potential dream. Various figures have been banded about including:

- 45% of users are "professionals"
- 56% are aged 21 - 30
- 80% are male
- the median income is US$54,000
- users spend over an hour on-line on average

The 'Internet' concept was first conceived in 1964 by Paul Baran at the Rand Corporation in America. He postulated an uncontrolled network which, by having no built in reliability and a totally distributed structure, would enable it to survive the massive destruction of a nuclear war.

The National Physical Laboratory in the UK set up the first test network on these principles in 1968. The Pentagon's Advanced Research Projects Agency (ARPA) funded a more ambitious programme in America in 1969. By December of that year there were four nodes and the ARPANET was born. Growth came quickly and by 1977 other networks were being connected.

Although originally intended for remote computing, much of the use of the Internet has always been for the exchange of news and personal messages. It also became the province of those wishing to explore the new found freedoms of computers. These were the true 'hackers' in the time before the word was corrupted to mean people who break into systems maliciously.

Most of the world's leading hackers started on the Internet and the trend continues. It is not therefore an area for hype, it is serious stuff. It is perhaps worth also noting that at the height of their 'infamy' (1988–1990) the Legion of Doom hacker group were predominantly teenagers.

Primary Problems

In looking at the Internet, there are a number of primary problems which become obvious very quickly.

Originally 'availability' was the purpose of the Internet and so, although the route a message takes can seldom be predicted, it does normally arrive. Given this background however it is interesting to note that at least one service provider only guarantees delivery to the Internet and not to the addressee.

'Confidentiality' and 'integrity' are not part of the network culture and it is the responsibility of the system user to provide appropriate and sufficient controls to safeguard their information.

Given the above, what chance is there for using the features of the Internet, which everyone seems to agree are very rich?

Essentially, if you want to communicate through the Internet in confidence, then take a leaf out of the hackers' book, encrypt!

There are plenty of software encryption options available, from DES or RSA downwards. The more common approach seems to be the use of public key encryption which enables you to publish a key for others to use. If you wish to be more advanced, try sending a GIF picture file with the message encrypted within it.

Underlying Architecture

The biggest perceived risk to Internet connected users is that of the underpinning architecture. Chiefly because they are below the normal 'access control' level these underlying transport layers are not considered as part of most people's security.

To consider this problem, it is necessary to look at the Open Systems Interconnection (OSI) seven layer model. Under this, there are seven distinct layers:

Layer	Level	Description
7	Application	Provides end-point services such as transfer, network management, transaction server.
6	Presentation	Provides code and syntax compatibility
5	Session	Provides session establishment, termination and recovery.
4	Transport	Provides acknowledgements and flow control between end-points.
3	Network	Provides routing and relaying when end-points are not physically adjacent.
2	Data Link	Provides reliable error-free transmission by organising digital traffic into logical frames with error detection and flow control.
1	Physical	Provides the ability to send/receive unstructured digital traffic over a physical channel.

As would be expected, each of these layers is dependent on the one beneath to provide the appropriate support services. The ones of key interest in this paper are layers 3 and 4 which provide the basic network and transport connections. At level 3 is the Internet Protocol (IP) whilst at level 4 is the Transport Control Protocol (TCP). Together these form the well-known TCP/IP and enable the transfer of data between machines in different locations using different operating systems.

At the IP layer, data is built into packets with a 32 bit source and destination address, some option bits, a header checksum and a payload of data. Every packet stands alone and there is no guarantee that a packet will be delivered, delivered once only or in any particular order. There is also no check for packet correctness as the header checksum covers only that header.

When moving around the system a series of 'hops' may be taken. At this stage, the IP packets may be fragmented, move out of sequence or be duplicated. The control of assembling these packets back to the correct format is left to the next layer, TCP, which manages this by having sequence numbers in every packet.

Communications Weaknesses

TCP/IP is only the underlying mechanism for data interchange. Using these protocols are other communications processes which are weak and need to be controlled. These include:

USDP ***User Datagram Protocol***
Similar to TCP in that it uses IP to deliver packets. There is however less control in that there is no guarantee of delivery.

ICMP ***Internet Message Control Protocol***
A low level mechanism used to influence the behaviour of TCP and UDP connections. Programs exist to exploit this protocol and redirect messages or tear down connections.

SMTP ***Simple Mail Transport Protocol***
Transports 7- bit ASCII text characters for electronic mail using a simple protocol. It does not provide authentication of the original sender of any mail based on it. One of its most common appearances is in the program 'sendmail' which often runs as root and therefore violates the basic computer security tenet of minimum trust.

Telnet
Provides simple terminal access to a machine. Most such sessions come from untrusted machines. The password and the terminal session are available to prying eyes and indeed the program can be hacked to record username, passwords and other details of the session.

Internal Issues

For any organisation that considers joining the Internet, there are a few points to consider, apart from security. The first is, how much time are employees allowed to spend on the net?

As the Internet is a 24 hour 7 day a week operation, staff could log in at any time and browse other sites looking for information for business purposes. If however they are logging on to join an on-line chat session (IRC – Internet Relay Chat), they could spend hours just reading others' comments and adding their own with no appreciable business content. Another point arises here and that is who do your employees speak for? Your company name may be part of their address and anything they say could therefore be deemed to be your company's policy!

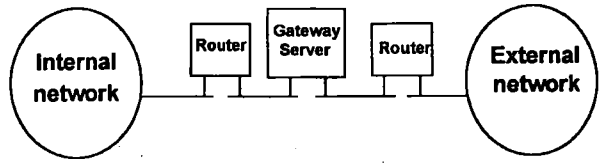
Some companies do in fact provide a standard e-mail 'trailer' for all users which points out that the views expressed are those of the writer not necessarily the organisation.

Naturally there are the standard problems of downloading programs and data. These include the perhaps excessive use of company resources (telephone lines and data storage), the dubious nature of some of the material available and the risks of viruses. There are other issues of software licensing and the dangers of overwriting valuable company data.

Firewalls

There is no doubt that the term 'firewall' has become more synonymous with Internet security than any other concept. For the sake of completeness, it will be dealt with briefly here.

It relies on the physical separation, as far as possible, of the Internet from any company's internal networks. A schematic of the concept appears below.



Firewall Concept Diagram

The basic problem is one that was discussed earlier, the TCP/IP weakness. This is not addressed by most access control systems and effectively allows an attack from any external network to come in underneath the primary system defences. This is because any normal gateway to the external world allows a whole range of accesses to come in and go out with no hindrance or control. All that a firewall does is to put effective filtering in place to prevent unwanted messages coming in and reduce significantly the likelihood that external attacks can capitalise on outgoing messages.

It is worth also pointing out that, yes you can pay £15,000 or more to purchase a firewall from a reputable company. You can also buy a cheap PC and download the software, free of charge, from the Internet. The phrase caveat emptor springs to mind.

International Laws and Controls

Given that the Internet spans national and international boundaries, what controls are there upon it? Essentially the only controls are those that the Internet community itself recognise.

In realistic terms, anyone breaking into the Internet from, say, England only commits a crime if they attack a UK based system. An attack on an American based or Japan based system would not commit a crime within the UK. It will commit a crime in America or Japan, but their jurisdiction does not extend to England. It is true that temporarily their influence could be brought to bear through international police links, but this is going to be dependent on three factors:

- the extent and nature of their own legislation,
- the type of crime committed, and
- the degree to which they are prepared to share information with another country.

In the first instance, very little of the computer law enacted covers every eventuality or is fully tested through the courts. Data privacy legislation is a case in point as this is notoriously patchy throughout the world. The second aspect is that is it worth pursuing the criminal anyway? Although the eyes of the law are now more focused on the Internet it is probably due more to the allegations that drug dealers use it as a communications channel than to the activities of the hacker community.

The third point is an interesting one. If it is assumed that the law is there and the crime is worth pursuing, how much co-operation is there when competing intelligence agencies may have to exchange sensitive information with one another? In addition, do these favours stack up?

Internet as a Marketing Tool

Much of the media interest on the Internet is how it can be used for buying and selling. The 'virtual mall' being but one term coined to describe it.

One route towards selecting the goods required is to instruct "agents" which are software programs designed to search and locate whatever is required. Intelligent agents would take this one stage further by obtaining alternative goods of the type the user prefers if the original item is not available. Capturing or copying these agents and then interrogating them would provide an invaluable source of marketing and personal detail which could be used by the criminal against the buyer. Similarly, amending the agents' brief could cause severe problems as incorrect goods are obtained or one 'shop' obtains all of the business.

The members of the Internet are not beyond protecting themselves when exposed to what are considered inappropriate or unethical advertising practices. A legal firm in America sent to all the addresses it could an advertisement for its services. The response was a classic 'denial of service' attack in that the mailbox of the offending company was flooded with so many spoof messages that it could not cope and was closed down.

Another risk area for network marketing is that of payment for services received. Credit cards are the obvious form of currency, but this information can be captured in transit across the network as well as the database on which it is held being vulnerable to attack. It is not uncommon to see credit card details for sale on the hacker boards.

It was reported in March 1995 that Visa card validation codes had been compromised by the release, across the Internet, of an internal Visa document 'Second Generation Authorization Formats'. This document was in fact published in Phrack Magazine dated September 1994. This magazine, which is a well known hacker publication, is now edited by one of the former Legion of Doom members.

Hackers

The Internet is full of them - or so it is popularly believed.

In reality, it is unlikely that a majority of the 30 million users spend their time in this way. There is however, a very active hacker community. Some of them are helpful and some are not. Nowadays, the latter group is most likely to be funded by other sources and therefore have the skills and other needs to undertake significant system break-ins and espionage. Noticeably these 'professional' hackers mistrust everyone including their own - there is far less knowledge sharing and co-operation than before.

It is also true to say that most of these hackers are UNIX experts and their preference is therefore for that system. Do not be complacent with an MVS or VME system, there are bound to be a few experts in every operating system, but your chances of sustaining a 'hit' should be smaller.

The Internet is rich in tools to aid the hacker community with the latest notable release being SATAN (Security Administration Tool for Analysing Networks) which helps to probe for security weaknesses on networks. As will be realised, any tools that help the hackers can also be used for the 'opposite' purposes by the security community.

In attacking systems, it is not unknown for hackers to move from one site to another in a series of hops designed to confuse any tracing of their activities. At each of these intermediate sites, the hacker will probe and penetrate the system sometimes just to provide a safe haven, but often to steal from, damage or disrupt that particular organisation. So although a company may not be a prime

target of attack, it needs defence in order to prevent itself being caught up in somebody else's problem.

Protection from Hacking

There may not be much that can be done to keep the determined hacker out, particularly one backed with someone else's money and resources. There are however a few steps which should be taken to reduce the risks:

1. In the first instance, a firewall is essential. This will protect your organisation from the major threats. It does however need to be constantly reviewed to ensure it continues to meet your needs.
2. Intruder attempts need to logged and these then need to be reviewed. There is a lot of work in this and it will only catch attackers it will not pick up those who are 'sniffing' around to test your defences.
3. Ensure that you have the most up to date versions of communication or defence software. Much is known about the weaknesses of old versions and how they can be exploited.
4. Reduce the amount of information publicly displayed about your site on the Internet to the minimum possible.
5. Create your own login and password screen wording. It is a big help to a user to see a familiar login screen as it will tell them what kind of system they are attempting to penetrate.
6. Insist on strong passwords being used and have them changed frequently.
7. Make use of challenge/response one time password generators for staff accessing your network from external points. This will reduce the likelihood of any passwords being compromised.
8. Put up the warnings about authorised access only. Not a great deterrent but could be useful if it comes to court.
9. Insist on secure destruction of company documents. Your blank headed notepaper could be used for fraud, but your telephone list quoting names, numbers, job titles and perhaps e-mail addresses, could be a goldmine for the information thief.
10. Ensure that your users are aware of security and the reasons for it. Too many attacks succeed because a user gave away a password. Remember, 'social engineering' is a hacker's greatest weapon.

It may be a long list but it is mostly commonsense and largely cheap!

Audit Implications

This paper has dealt with most of the control implications of joining and using the Internet. It is of course up to each organisation to interpret these and any other guidelines in the way best suited to itself. In this aspect, audit has a key role to play particularly in advising management on the extent of the risks that are faced and how they can be minimised.

In practice, the Internet is merely a service tool and the service it provides, its resource costs and the benefits it yields all fall under the aegis of audit to review in the manner of any other service. The fact that it is an open invitation to outsiders to try and look in at your company's 'goodies' must not be overlooked and the access logging and other protection mechanisms should always be given high audit priority.

Summary

Connecting to the Internet is another business decision and audit and security staff need to be aware of the strengths, weaknesses, opportunities and threats of it in the same way that they are for other services in order to provide the appropriate advice for management and guidance for users.

Forewarned is forearmed!

Bibliography

Anon. *Computing*, 23 March 1995

Anon. *Eurosinet, Database and Network Journal* volume 16 number 4

Anon. *Internet*, January 1995

Anon. *Phrack Magazine*, volume 5 issue 46 September 1994

Aime J Bayle. *Security in open system networks: a tutorial survey*, Information Age volume 10 number 3 July 1988

William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security*, Addison Wesley, 1994

Dr Brian Neale. *Secure Connections to the Internet*, Digital Equipment Co. Ltd. (circa 1994)

Richard Sizer. *Data, Information and Networking*, Information Age volume 10 number 4 October 1988

Arlene H Rinaldi. *The Internet - User guidelines and netiquette*, Florida Atlantic University, September 1992

Bruce Sterling. *The Hacker Crackdown*, Penguin, 1992
Bruce Sterling. *Brief introduction to the Internet*, The Magazine of Fantasy and Science Fiction, February 1993

Clifford Stoll. *The Cuckoo's Egg*, Pan, 1990

Brian Wood, *Standards Download*, Government Computing, October 1987

SAFETY CRITICAL SYSTEMS

Felix Redmill

One of the areas in which some of our members are interested in is the audit of safety critical systems. As a member of the public, I am very interested in the controls over nuclear power stations, fly-by-wire aircraft and the railway signalling system, not to mention the myriad of other computer systems that keep us one step away from disaster. You may be interested to know that there is a specialist group which deals with such matters. Felix Redmill has been good enough to provide us with some information regarding this very important area. (Editor)

The 'safety-critical systems' domain, embracing software-based systems in safety-critical applications, is based on the blending of the expertise of professionals from a number of existing fields. Notably, these are safety engineering and software and systems engineering, but as safety-critical systems expand into almost every sector of industry, they demand input from other specialisms too, such as human factors, management and the quality discipline. Typically, practitioners from the various fields are proficient only in their own disciplines, and there is a need for the transfer both of existing technologies between disciplines and of new technologies into the broad safety-critical domain. In addition, there is an urgent requirement for system developers in all sectors of industry to be more aware of the safety implications of their products and of the need to employ the most appropriate technologies in their construction.

SETTING THE SCENE FOR A COMMUNITY CLUB

In 1989, the Institution of Electrical Engineers (IEE) and the British Computer Society (BCS) produced a joint report[1] on 'the problems arising from the specification, design and assessment of software for use in safety-related systems'. Among many recommendations which have since proved influential was the observation that 'a major factor affecting safety is a lack of awareness on the part of individuals and organisations of how and to what extent their work is safety-related'.

In 1990, the Joint Framework for Information Technology (JFIT), which had been created by the Department of Trade and Industry (DTI) and the Science and Engineering Research Council (SERC) in 1988, initiated a safety-critical systems collaborative research programme. Project proposals were invited, and in 1991 the first round of projects was approved. Projects needed to comprise a partnership between academia and industry and were chosen not only to cover a broad spectrum of technologies and phases of the life cycle, but also a variety of industrial sectors. One of the principles of the programme was that technologies developed should receive early trials in industry and, if successful, be quickly made available for more general use.

This needs for technology transfer and for raising awareness within industry created the climate for the formation of The Safety-Critical Systems Club.

INAUGURATION

In 1991 the BCS and the IEE, along with the Centre for Software Reliability at the University of Newcastle upon Tyne, were contracted by the DTI and SERC to set up a community club for technology and information transfer, and for raising awareness, in the safety-critical systems domain. The current author was engaged to be the club's Co-ordinator. The club was launched in May 1991 and 255 delegates attended the inaugural meeting in July of that year. When the funding period came to an end, at the end of April 1994, the club's membership was almost 2000.

THE CLUB'S OBJECTIVES

The club exists to facilitate information and technology exchange and to increase awareness in the safety-critical systems domain. It is recognised that in order to be successful in this, the club must attract not only engineers and technicians but also managers with decision-making responsibilities.

By facilitating communication across industry, the club seeks to:

- Increase the rate of dissemination of useful technologies;
- Prevent the spread of flawed technologies by the rapid communication of experience;
- Improve the industrial testing of new technologies;
- Bring industrialists together to plan feedback to academia and to co-ordinate the sponsorship of research. By facilitating communication between academia and industry, the club seeks to:

- Improve the choice and application of technology;
- Accelerate the feedback to academia of experience in the use of technologies;
- Improve safety-critical computer systems which are supplied to industry;
- Inform the choice of research topics and projects;
- Accelerate the correction and improvement of flawed but useful technologies.

SUCCESS IN MEETING THE OBJECTIVES

Newsletter

A newsletter is published three times annually and distributed to all members. Typical contents are:

- Feature articles on safety-critical systems and related matters;
- A calendar of events on safety-critical systems;
- A calendar of events on related issues;
- Calls for papers for future conferences;
- Reports on new products;
- Reports on government studies or initiatives affecting safety-critical systems;
- Comments by members on safety-critical issues.

Seminars

By the end of its fourth year of existence (April 1995), the club had held 16 one- and two-day seminars. The topics covered were:

- Inaugural meeting and introduction to safety-critical systems;
- Requirements for safety-critical systems;
- Education and training for safety-critical systems professionals;
- Safety-critical software and technology in the medical sector;
- Standards for safety-critical software;
- Human factors in safety-critical systems;
- Design for safety and reliability;
- Safety-critical systems in the nuclear sector;
- The safety case;
- Testing and Validation;
- Measurement of Safety and Reliability;
- Legal and Social Aspects of Safety-critical systems;
- Safety-critical Systems in the Transport Sector;
- New Technologies;
- Management for Dependability;
- Safety-critical Systems in the Medical Sector.

A full programme has already been planned for the remainder of 1995 and for 1996, and the 4th Safety-critical Systems Symposium will be held at Leeds on 6-8 February 1996.

The majority of the seminars are on topics of broad application. However, each year a sector-specific event is held in order not only to facilitate communication within the sector itself but also to allow participants from other industry sectors to benefit from that sector's technologies and lessons.

Average attendance has been about 100, and the questionnaires completed by delegates show positive feedback on both the quality and immediate value of the events.

The speakers at the first five seminars, all experts in their fields, were invited to prepare chapters for an edited book. Twenty-two speakers responded, and the resulting volume[2] was published by Chapman and Hall in 1993.

Annual Symposium

The first Safety-critical Systems Symposium (SSS '93), initiated and organised by the club, was held in Bristol in February 1993 and attracted 190 delegates. The 19 papers presented covered a broad spectrum, many reporting on research projects from the DTI-SERC safety-critical systems programme. Moreover, a feature of the event was the number of discussion sessions which provided opportunities for questioning, information exchange, and the generation of new ideas. There was also a poster session in which research projects were exhibited and explained so that industry and other researchers could get a feel for the technologies in preparation. The proceedings of the Symposium[3] were published by Springer-Verlag in time for each delegate to receive a copy at the event. They are now available from the publisher.

The second and third Safety-critical Systems Symposia were held at the Belfry, near Birmingham, and Brighton respectively. They followed the pattern of the first, offering invited papers on both current research and industrial practices (such as risk management), extensive discussion, and a forum for a wide-ranging exchange between industry and academia. The proceedings of both[4,5] were published by Springer and are still available from the publisher.

The average attendance at the three symposia is 175.

Ad Hoc Activities

The club has also participated and assisted in a range of supplementary activities. It has co-sponsored events, assisted in the organisation of workshops, given advice on safety-critical issues, held poster sessions at events, brought together potential participants in collaborative projects, and given publicity to safety-critical matters. A recent initiative has been the creation, jointly with others, of a risk and safety analysis group, the purpose of which is to facilitate the adapting of existing risk analysis methods for use with software-based systems and to encourage the use of the resulting adapted methods.

FINANCES

The contract with the DTI and SERC provided for funding of the club over three years, diminishing from full funding to nothing. This required the club to become self-sufficient by the fourth year. Although good attendance at club events has provided a modest surplus, this is insufficient to cover all running costs, so in early 1993 the club management were forced to ask members to pay a subscription. By the time subscriptions were requested, a membership of 2000 had been built up, demonstrating the need for and interest in the club. A fair proportion of that membership have subscribed, but more paying members are required to cover the club's costs.

A distinction has therefore had to be made between subscribing members and those merely on the mailing list. Only members receive the newsletter and, in addition, members pay a reduced charge at seminars, the reduction being equal to the membership subscription - so it is worth subscribing.

MANAGEMENT

Although the financial sponsorship of the DTI and SERC has expired, all the institutions formerly involved with the club have retained their interest and continued their support. Indeed, they participate actively in the club's strategic planning. Oversight of the club's affairs and the setting of direction is carried out by a Steering Group comprised of industrial members and representatives of the Department of Trade and Industry, the Engineering and Physical Sciences Research Council, the Institution of Electrical Engineers, the British Computer Society.

Given this overseeing body, day-to-day management of the club's affairs is handled by the Centre for Software Reliability at the University of Newcastle upon Tyne, and technical organisation of the club's seminars and symposia and the editing of the newsletter are carried out by the Co-ordinator.

THE FUTURE

In its four years of operation, the Safety-Critical Systems Club has staged nineteen successful events, published four books, and further facilitated the raising of awareness and the transfer of technology by the publication of a regular newsletter, the co-sponsorship of events, and the provision of advice.

The large membership and the high attendance at events demonstrate the need for the club, and the feedback suggests that the club is fulfilling the need. Yet, there are many engineers and managers in the safety-critical domain who would benefit from greater awareness and a familiarity with the latest technologies, but who are not aware of the club or its activities. It is the club's policy to continue to provide its present services and to publicise its presence so as to serve an increasing proportion of the safety-critical systems community.

ACKNOWLEDGEMENT

An earlier version of this article was published in the Computer Bulletin. Acknowledgement is made to the British Computer Society.

REFERENCES

[1] Institution of Electrical Engineers: Software in Safety-Related Systems. A Report Prepared by a Joint Project Team of IEE and BCS, IEE, October 1989.

[2] Redmill F and Anderson T (Eds): Safety-critical Systems - Current Issues, Techniques and Standards. Chapman and Hall, London, 1993.

[3] Redmill F and Anderson T (Eds): Directions in Safety-critical Systems - the Proceedings of the First Safety-critical Systems Symposium. Springer-Verlag, London, 1993.

[4] Redmill F and Anderson T (Eds): Technology and Assessment of Safety-critical Systems - the Proceedings of the Second Safety-critical Systems Symposium. Springer-Verlag, London, 1994.

[5] Redmill F and Anderson T (Eds): Achievment and Assurance of Safety - the Proceedings of the Third Safety-critical Systems Symposium. Springer-Verlag, London, 1995.

Information on the Safety-Critical Systems Club may be obtained from Mrs J Atkinson, The Centre for Software Reliability, Bedson Building, The University, Newcastle upon Tyne, NE1 7RU, UK; Tel: 0191 221 2222; Fax: 0191 222 7995.

The author is the Co-ordinator of the Safety-Critical Systems Club. He is a consultant in Software Quality and Project Management and may be contacted on 0181 883 0789.

INSTITUTE OF INTERNAL AUDITORS REDESIGN THE QICA QUALIFICATION

David F Bentley, Chairman QiCA Committee, IIA-UK

The Institute of Internal Auditors – United Kingdom and Ireland – has placed a particular emphasis over the past twenty years on the development of approaches to the audit of computer systems. It also introduced a specific qualification for computer auditors in 1981, in an attempt to provide a yardstick against which to measure the knowledge of auditors.

We have recently reviewed our approach to this qualification and made a number of changes which should make it more attractive to a wider community of auditors.

When the qualification was first introduced, its syllabus was closely related to information technology and its impact on the audit process. Over a period of years, particularly in the late 1980's, it extended the syllabus to include a number of papers from the MIIA professional qualification, and became, as a result, a broader internal audit qualification.

The Institute has now decided to reverse the approach as part of a wider review of its professional qualifications. The revised QiCA regulations now require participants to pass two three-hour examinations and provide evidence in a logbook of practical experience covering a number of specific areas over a minimum period of two years. In addition, on passing the examinations, participants will be awarded a Certificate in Computer Auditing Theory.

EXAMINATION SYLLABUS

The examination syllabus consists of two papers, a first level paper on "Information Systems Auditing" and a second level paper on "Specialist Information Systems Auditing".

"Information Systems Auditing"

The syllabus for "Information Systems Auditing" has been revised and will cover:-

- Control in IT systems
- IS Strategy and Development
- IS security operations
- Software
- Basic CAATs
- Control and audit of application systems
- Communications and Networks
- End-User Computing
- Computer Misuse and the Law

"Specialist Information Systems Auditing"

This paper focuses on some of the more technical issues and demands a detailed understanding of the principles and practices of information systems auditing at a practitioner level. Candidates are expected to be able provide examples drawn from their own experience on how systems software and hardware deals with specific control issues.

In recognition of the fact that an auditor's scope of work may be determined in part by the IT environment in which he or she operates, the examination syllabus is based on a number of options. It currently requires candidates to select questions from three of the following five specialist areas:-

- Operating Systems and Systems Software
- Security, Contingency Planning and Recovery
- Networks and On-Line Processing
- Database Systems
- Microcomputing

It is planned to change the specialist areas in 1997 to the following:-

- IT Management (including strategy, project development, systems development, audit automation)
- Systems Software (including operating software, database software, access control software and microcomputing software)
- Security and Contingency Planning
- Networks and On-line Systems
- Auditing Applications and Advanced Systems

Under this revised syllabus, IT Management will become a compulsory topic and candidates can chose two of the other four options.

PRACTICAL EXPERIENCE REQUIREMENTS

The practical experience requirements require authenticated evidence of work experience covering a range of activities, comprising of at least 1600 hours over a minimum of two years. This must include at least 250 hours on basic topics, for example:-

- the use of the computer as an audit tool
- the audit of an operational system
- the audit of a system under development
- some installation audit work
- the audit of PC -based systems

There must also be evidence of work covering technical audit reviews from at least three of the topics covered in the advanced

syllabus. There should be a minimum of 250 hours in each of the three areas nominated. Detailed guidance is provided on the completion of the experience log, which includes examples of the types of work which can be included, and the level of detail required to enable the QiCA Committee to judge the appropriateness of the work experience.

TUITION AND EXEMPTIONS

The normal starting point is for a candidate to enrol for a course of tuition for the paper on "Information Systems Auditing". There are a number of tuition centres in the UK and Ireland offering courses of study for this paper and IIA-UK also runs its own Distance learning course.

There is no requirement for a compulsory course of tuition for the second level paper on "Specialist Information Systems Auditing". The Institute will produce a detailed syllabus, reading lists and specimen examination papers and suggested answers. The Distance Learning material produced for the current syllabus, which can be purchased, will be of value in preparing for the examination.

Holders of the MIIA, CISA and MBCS qualifications will be granted exemption from the first level "Information Systems Auditing" paper. There are no exemptions from the advanced paper.

Experienced data processing professionals or managers with at least three years experience related to IT auditing may apply for exemption from the compulsory tuition requirements applicable to "Information Systems Auditing".

CONCLUSION

IIA-UK recognise that it is important that internal auditors have the necessary skills to audit in an information systems environment, and the QiCA programme provides a study and examination process to measure the knowledge of its participants. The qualification is not restricted to internal auditors, and external auditors who need to undertake audits of a technical nature should find the qualification of value.

It is intended to introduce continuing professional development requirements in the future.

An information pack on the qualification is available from IIA-UK, 13 Abbeville Mews, 88 Clapham Park Road, LONDON SW4 7BX (Tel 0171-498 0101).

Rob Melville, who edited the Journal for three years writes . . .

VALEDICTORY

In what seems like another century, but was really only 1990, a colleague approached me about a new journal. I'd recently joined City University Business School as a lecturer in internal auditing and the new journal was for the Computer Audit Specialist Group. The group itself was not new to me, I had been meaning to join it since it was the old 'ABC'. But the idea of working with some of the most influential figures in the profession was too hard to resist. My colleague introduced me to Ginny Bryant, I volunteered to write a quarterly piece and that I – thought – was that. Over the next year or so, Ginny and I worked as joint editors and we had a mixture of spectacular production failures and equally spectacularly influential articles. Somewhere along the way I took over completely, we got the production 'outsourced' (in other words, hard up students were paid to stuff envelopes) and we started to get a real repuation as a high class specialist journal. Later, we made the crucial decision to get professional layout and distribiution. Today, the journal is a product of which the group can be genuinely proud. It has been a wonderfull rewarding time for me, but now it's time for new blood.

Reviewing the changes over the last five years has been interesting. Back then computer auditors still had strong links to the mainframe, systems developments were mainly traditional 'life cycles' and the pentium chip was still a dream. I remember writing an article for the BCS Bulletin about the future: networks, POS, telecommuting and systems development methodologies were key concerns. Now we have BPRE, downsizing, incremental developments and most of all, we have end user power. Back in 1988, I tried to get colleagues interested in auditing micro's, as part of their ususal systems reviews. The reaction was not positive and it got worse when I wanted my team to do their own word processing! The birth of GUI's has put almost undreamt of power into the hands of users, and easy access to the net has enabled any journalist in search of a cheap piece to discuss the net as a pro or con, or to raise paranoia about Satan (in effect, a perfectly reasonable piece of software but with a dodgy acronym).

My closing piece was elicited, agreed to and sent via e-mail. Those of you with long memories will remember that some years ago the journal was among the first ever to use e-mail to request, edit and accept a contribution. We can be certain that John Mitchell with his new hat will continue our moves towards state of the art.

MEMBER PROFILES

Edited by Jenny Broadbent

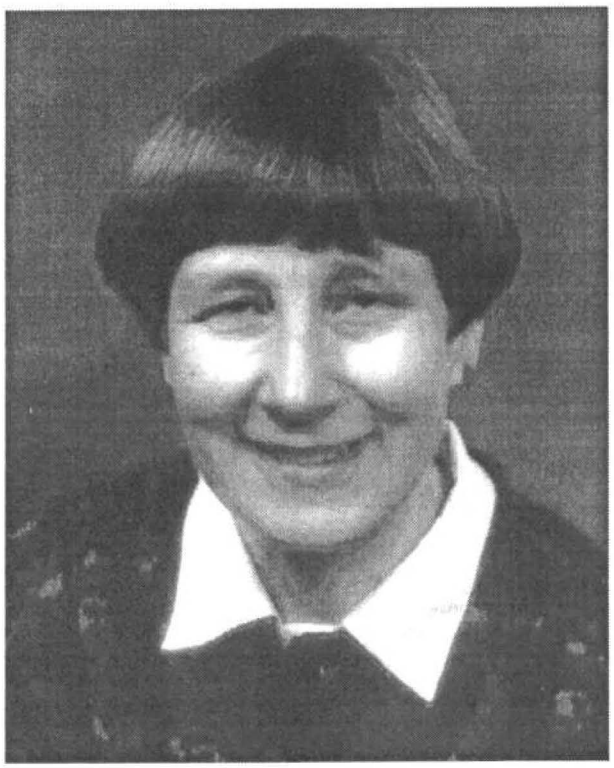
This column will bring you details of our members.

If you would like to nominate someone for inclusion, then please contact Jenny.

ALISON WEBB

Current Position: Independent Computer Audit Consultant

CASG Involvement: Chairman



Alison is an independent computer audit consultant, based in Cambridge. She divides her time between auditing large IBM mainframe systems and giving general advice and assistance to firms with business computer needs.

She trained as an accountant with Pannell Kerr Forster in Derby before joining the computer audit department of KPMG Peat Marwick Mclintock in London. There, she specialised in the audit and security of large systems, including audit interrogation, system and application software reviews and installation reviews.

In 1989 she joined Peters Elworthy and Moore, an independent firm of Chartered Accountants based in Cambridge. There, she managed a general audit department (and tried to remember what she'd forgotten about company taxation!) but her special responsibility was to develop computer audit in the firm. She introduced in-house file-interrogation techniques and worksheets and questionnaires based on simple risk assessment to evaluate security and controls in small and medium sized computer installations and systems, as well as guidelines for PC security.

In 1990, computers triumphed over corporation tax, and Alison left general practice to concentrate on computer consultancy.

JOHN SILLTOW

Current Position: Group Security Manager – The Woolwich Building Society

CASG Involvement: Member of the Journal Editorial Panel

I was born at an early age, the son of a great man, as my father always said.

My education was unremarkable except for discovering the differences between girls and boys before discovering bicycle sheds and therefore being unable to utilise the knowledge! I was reminded recently that one of my earliest remarks after going to school was

to the effect that the teachers do not know anything as they keep asking us questions. That incisive reasoning could perhaps explain my exam results.

When I left school, I took a strategic career decision and joined the Civil Service (for the quill pens, pension and machismo you understand). Early on I issued flight crew licences, manned merchant ships and did all sorts of odd things until applying for a job in Washington and found myself posted to Melbourne, Australia (the word is deported – *Ed*). I worked on the commercial aviation side, had a great time and learned a lot, not the least of which was how many beers it took to make me fall over.

After that, my career took a serious downturn in that I returned to England and joined the DTI's internal audit unit! The worst thing was that I actually enjoyed it so much I was promoted! After a couple of years, I transferred to the British Library's fledgling internal audit department and took up such things as computer audit and computer security. The latter under the guidance of Ken Wong.

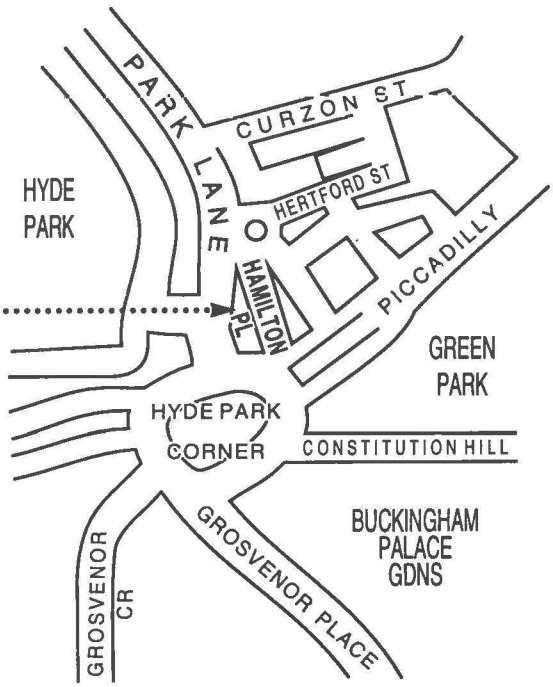
I zoomed through eight years in the Library (I'm a slow reader) moving from audit to project management to personnel and on to heading up their physical security section. I then took a major career decision (based on money) and threw in my lot with the Woolwich as a computer auditor specialising in microcomputers. My time in that job was marked by the number of reports I wrote which criticised computer security so it will be of no surprise to work out where they transferred me to!

Thus 1990 marked the return of the prodigal son to computer security. I admit to not having looked back since. My role has grown over the years and I am now responsible for the strategic direction of security throughout the Woolwich Group. It's an occupation I guess you love or hate. Fortunately for me, I love it. Perhaps it's being on that knife edge of good or evil, maybe even because there is seldom only one 'right' answer, but more likely it's standing up in front of people like you and discussing the issues.

Thanks for helping me enjoy it.

Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ



CASG Editorial Submission Deadlines

Spring Edition	14th February
Summer Edition	14th May
Autumn Edition	14th August
Winter Edition	14th November

British
Computer
Society

PLEASE RETURN TO
Jenny Broadbent
Membership Secretary
Room C309
Cambridgeshire County Council
Shire Hall
Castle Hill
Cambridge CB3 0AP

Membership Application

(Membership runs from June to the following May 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 delegates)* £75

* Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal and attendance at our meetings *(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: _____

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)
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 CASG"
AND RETURN WITH THIS FORM TO THE ADDRESS SHOWN ABOVE

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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)

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)

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)

PROFESSIONAL CATEGORY:

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

British
Computer
Society

Management Committee

CHAIRMAN	Alison Webb	Independent Consultant	01223 461316
SECRETARY	Raghu Iyer	KPMG	0171 311 6023
		Email: raghu.iyer@kpmg.mark400.gb	
TREASURER	Bill Barton	Independent Consultant	01883 623355
MEMBERSHIP SECRETARY	Jenny Broadbent	Cambridgeshire County Council	01223 317256
JOURNAL EDITOR	John Mitchell	LHS - The Business Control Consultancy	01707 851454
		Email: jmitchell@lhs.win-uk.net	
MEETINGS	Paul Howitt	Tesco Stores Limited	01992 644250
	Jim Ewers	Hertfordshire County Council	01992 555328
	John Bevan	Audit &Computer Security Services	01992 582439
	Geoff Wilson	Independent Consultant	01962 733049
	Allen Brown	Independent Consultant	01803 327874
	Diane Skinner	Audit Commission	01179 236757

Membership Enquiries to:

Jenny Broadbent
Room C309
Cambridgeshire County Council
Shire Hall
Castle Hill
Cambridge
CB3 0AP

Tel: 01223 317256