casg Computer Audit Specialist Group

JOURNAL

VOLUME 7 NUMBER 4 SUMMER 1997

ISSN 0961-9348

The British Computer Society

## Technical Briefings 1997/98

**For more details of all Technical Briefings, and details of costs and registration, contact Jean Brown, on 01803 872775**

**IT and the Law**
**15 October 1997 at the Royal Aeronautical Society, London**
Chairman: Willie List, BCS Security Committee

| | |
|---|---|
| The Procurement Process | Rosemary Boyle<br>Cambridgeshire County Council |
| What goes wrong | Hilary Pearson, Bird and Bird |
| What to put into the contract | Alan Laing, Oracle |
| Shrink-wrap licensing - Data protection implications | Christopher Millard, Clifford Chance |
| Expert Witness in IT | Ron McQuaker, President, British Computer Society |

**Electronic messaging**
**27 January 1998 at Chartered Accountants' Hall, Moorgate Place, London**
Chairman: Steve Hinde

| | |
|---|---|
| Connectivity and the accountant | Malcolm Marshall, KPMG |
| open.gov: the electronic delivery of government services | Matthew Bishop, Cabinet Office |
| Uses and abuses of e-mail | Daniel Strawson, Electric Mail |
| Electronic Lodgement | Brian Handley, Project Officer, Electronic Lodgement, Inland Revenue |
| Commerce and the Internet: Auditing Implications | Freddy MacMarne, NatWest Electronic Markets |

**Looking beyond the Millennium**
**28 April 1998, at the Royal Aeronautical Society, London**
Chairman: Martin Robinson, IIA

| | |
|---|---|
| Auditing a RAD Project | Jennifer Stapleton, Vice-President of the BCS, and Chair of the Technical Board |
| Major Projects: what can go wrong | Brian Helbrough, Imago |
| Using the benefits of hindsight - the role of post-project analysis | Arnold Kransdorff, Pencorp Ltd |
| Penetration testing | John Austen, BA FBCS<br>Computer Crime Consultants |
| Fraud investigation and internal security | Tom Mulhall, BT |

**Followed by the Annual General Meeting.**

# Contents of the Journal

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 Post Script,
Tring, Herts.

# EDITORIAL

My comments in the last edition about the lack of auditors putting pen to paper did at least produce one response (see letters), even if it was to describe all the reasons why the readership are unlikely to do so! That aside the academics are at least willing to have a go and this edition contains an article from Andrew Hawker on the problems of prediction and one from David Chadwick on the problems of teaching students about spreadsheet control. David has thrown down the gauntlet by asking for suggestions on how to improve teaching in this area. Come on you practitioners, help our university cousins by divulging your tricks in auditing spreadsheets.

We also have an amusing article from the partner of a computer auditor on the trials and tribulations of living with one and short articles on software upgrades and outsourcing. Paul Howitt continues his Hotel & Restaurant Watch column and our BCS pages include an article from Hazel Roberts, our BCS Librarian, on the new role of the Cyber Librarian. The BCS Security Committee is once again asking for your help on a number of issues, while Colin Thompson brings us up to date on various initiatives from our parent body.

I spent a pleasant week in New Zealand last month attending EDPACS 97 which is run by our sister group the Information Systems Audit & Control Association (ISACA). The conference message was consistent from a whole range of speakers. Control Self Assessment to help with the corporate governance problem, the risk from information warfare as our dependence on the Internet increases and the need to become involved in system development at an early stage. You will notice that our Technical Briefings for next season cover the procurement process, connectivity and fraud investigation which is a pretty good mirror of the main EDPACS themes and indicates that the problems are generic in nature.

The Audit Commission is once again conducting its survey of fraud and abuse. You will find details inside this edition. If you have not received a survey form, or have not yet returned the one you have, then please do something about it. To quote the motto of the Institute of Internal Auditors, 'progress through sharing' only works if people genuinely share their experiences.

Our first Technical Briefing of the year is on the 15th October. Renewal invoices for next season will shortly be landing on your desks. Remember, no renewal, no discount. Have a good summer.

**John Mitchell**

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

# Chairman's Corner

**Alison Webb**

This issue follows our Annual General Meeting and the subsequent committee meeting that sets the agenda for the new season. This year, we are continuing with the Journal, of course, and with the Technical Briefings, which are already at an advanced stage of preparation. You'll find details of them on the front cover of the Journal.

As well as these regulars, we are trying two new initiatives this quarter, which I hope will be popular enough to make part of our regular services.

The first relates to the Technical Briefings. We taped the Briefing on "Systems Development: Adding value by Audit" on 15 April 1997, and as an experiment, we are offering copies of the tape, plus copies of the notes, for sale at £30.00 plus VAT. If you'd like a set, please send your cheque for £35.25 made payable to BCS CASG to me, Alison Webb, 30 Kingston Street, Cambridge CB1 2NU. You know the rules now (some people are probably still nursing their wounds from 15 April): don't even think about asking me for an invoice!

The other initiative stems from our position within the BCS. Public pronouncements on security are made by the BCS Security Committee, and John Bevan and Allan Brown are our CASG representatives who keeps track of what they are doing. A lot of serious stuff lands on the Security Committee's table, and we feel that in some areas especially, CASG members could (and indeed should) make a very valuable contribution to the debate. John is therefore organising the first of what we hope will be a series of relatively informal evening meetings in London, where members of CASG can discuss with someone from the Security Committee topics of mutual interest, and where our members will get an opportunity to put their points of view forward. Depending on timing, you may already have been circulated about this, but we hope that if you can, you will support it. (I apologise to people some distance from London, but at the moment, we can't offer any alternative venues).

We will circulate everyone with details, but in the meantime, please ring John on 01992-582439 if you'd like to know more.

# Prophets and Losses

## Andrew Hawker

In 1979, physicist Dr Brian T Brady predicted that, two years later, a major earthquake would occur off the coast of Peru. His prediction was rejected by the US National Earthquake Prediction Evaluation Council, but nevertheless caused widespread alarm in Lima, which was expected to bear the brunt of the damage from a tremor around eight on the Richter scale. Leading figures pointedly arranged visits to Lima on the designated date, June 28th, to demonstrate their solidarity with NEPEC's conclusions. Peru's population held its breath. Nothing happened[1].

This is not of course the way things turn out in Hollywood movies. Invariably, the audience knows for a fact that man-eating sharks are on the rampage, aliens are crawling out of pods at the dead of night, or life as we know it is about to be obliterated by a huge asteroid. No sane scriptwriter is going to base a narrative on the idea of the prophet as a crack-pot. If nothing happens, it will always be because of some heroic interventions, usually by the same visionary who drew attention to the problem in the first place.

Computer auditors are occasionally called on to make prophecies. More enlightened management may actually invite them to. In the more contentious cases, the auditor may feel impelled to issue dire warnings about dangers ranging from discrepancies in data to the collapse of the whole business. Framing prophecies is necessarily a difficult art, and, as Dr Brady found out, you have to be conscious of two principles at work: (i) it may be necessary, in order to get any attention, to frame your prophecy in clear and dramatic terms; and (ii) if your prophecy turns out to be wrong, most of your credibility will bite the dust alongside it.

It was with this in mind that I read the contribution made recently by Vesselin Bontchev to the debate on macro viruses[2]. Bontchev is not exactly making a doom-laden prophesy, but after thirty-two pages of his thoughts about the design weaknesses of Word for Windows, the practical effect was much the same. I confess I have become a lot more thoughtful about exchanging Word documents with other users, and have taken to sending .TXT instead of .DOC files. Perhaps, as with eating beef, I will eventually revert to old habits, but the article raises some nagging questions.

Bontchev describes how he has infected his own Word system with numerous pieces of marker code, designed to show whether an action could be commandeered by a macro virus. He has reached the point where even a single keystroke can trigger such a warning. He suggests that macro virus writers will be well aware of such possibilities, and that there are a number of other vulnerabilities which he can only hint at, since to explain them would be to aid and abet the enemy.

At the back of his mind there are no doubt thoughts of the reaction which greeted the release two years ago of SATAN, which was criticised for putting powerful analytical software in the wrong hands. Tools designed to help the computer auditor will often, unavoidably, be capable of misuse by hackers and virus writers. An article such as Bontchev's, which seeks to alert the security community to the ways in which macro viruses could develop, may well inspire new forms of attack as well as helping people to strengthen their defences. On balance, I suspect most of us would prefer to be told about possible new threats, even if this increases the probability that the risks will actually materialise.

Apart from the ethics of disclosure on the part of virus experts, the other key ethical issues centre on the position adopted by Microsoft. For many years, DOS has provided the base for a flourishing industry in virus creation, not just because of its almost universal adoption in personal computing, but because the way it was designed, with its default search of the diskette drive and a boot sector which could be used as a launch base. This has made it ideal for virus transmission. Most of these vulnerabilities survived even when DOS was re-written and embedded in Windows. During all this time, Microsoft's stance was one of wringing its hands while counting the revenues as the licence agreements poured in. Thanks partly to the efforts of a flourishing anti-virus industry, we were all persuaded that viruses were as natural as the common cold, and treatable with the equivalent of a few packs of paracetamol. DOS could never have been made completely virus-proof, but it could, for example, have been made a good deal more pernickety about how it booted itself up. This would undoubtedly have annoyed some users. Microsoft simply ducked the issue, and the indirect costs of virus protection continue to escalate.

In the case of macro viruses, such indifference on the part of the company could be a lot more serious. Bontchev describes a prototype "Macro Virus Protection" option shipped to him by Microsoft. Besides being more than a touch naive (it simply advises if any macros are in use in connection with the document, leaving the user to determine whether they are malicious or not), the "protection" turns out to have a number of holes in it.

With the growing popularity of Microsoft Office and the emergence of Word as a de facto document standard, perhaps Microsoft should reflect further on the possible scenarios which could follow a loss of confidence on the part of their word processing customers. It is not just current documents which are at risk, but those held in archives. If key documents are rendered unreadable, a company may face heavy losses because it cannot introduce evidence to defend itself or cannot retrieve essential details of a contract. Even a document which does not appear to have been altered may become suspect, simply because it has been exposed to macro viruses. Responsibility surely lies with the provider of a widely-used software package to make every effort to make it virus-resistant. The alternative is a never-ending round of updates to detection software, efforts to reconstitute files, and the taking of extensive back-ups. All these activities generate substantial costs for customers.

Bontchev has couched his warnings in fairly cautious terms. He has not predicted a force eight earthquake. However, he has identified a large number of warning tremors, and, (if the metaphor can be stretched a little), there seem to be some major faultlines running straight through Wokingham and Seattle.

[1] R.S.Olson The Politics of Earthquake Prevention 1989 Princeton University Press

[2] V.Bontchev, Possible macro virus attacks and how to prevent them, Computers and Security, 1996 15:7 595-626.

*Dr Andrew Hawker lectures in information technology at the Department of Accounting and Finance, University of Birmingham. He can be contacted by email at the address: HAWKERA@css.bham.ac.uk*

# Computer Fraud and Abuse - the 1997 Survey

**Chris Hurford**

The Audit Commission is soon to launch the sixth triennial survey of UK computer fraud and abuse. All the previous surveys have come to be regarded as authoritative and reliable sources of information on the subject of computer fraud and abuse and have been widely quoted by research organisations and others with an interest in the extent and nature of computer crime.

But has the computer abuse scene changed over the past 18 years? The first survey of computer fraud and abuse in the UK was published in 1984 and it commented that "The risks of fraud and abuse will be all the greater if internal controls and internal audit are inadequate. Poor supervision and ineffective audit will almost certainly encourage the opportunity for large scale and long-running losses. Where the organisation sustains such an environment and still encourages the widespread introduction of computing, the risks will be considerable".

There seemed little improvement when the fourth triennial survey was published a decade later and reported "Now, as then, opportunities are still widespread and weaknesses well-known, but for a variety of undisclosed reasons, management do not impose adequate controls". That survey highlighted a number of trends in computer fraud and abuse and emphasised that organisations were facing a range of threats:

- an almost five-fold increase in reported virus infections;
- a 38 per cent increase in the number of frauds;
- an almost eight-fold increase in the use of illicit software; and
- a four-fold increase in instances of unauthorised private work.

Now three years on, will the picture be any different? Well much depends upon the effectiveness of internal control and of internal audit activities over the past three years. The media suggests that computer abuse is still a real threat with substantial losses being suffered by many.

As technology becomes more invasive, so the risk of its misuse increases. There seems little doubt that computer abuse is now well established and as the use of technology extends, the likelihood of deliberate acts of computer abuse will increase and the impact become much greater. While the tip of the iceberg may be identifiable, the greater and more significant impact may remain hidden.

Over the next month or so questionnaires will be distributed to heads of finance in the public and private sectors asking them to contribute to this vital data-gathering exercise. The Commission believes that it is important to understand the scale of the problem and to capture examples of the incidents which have occurred and the losses which have been suffered. By better understanding the nature of the risks, organisations should be better able to devise effective controls and safeguards.

Forecasting the results of surveys can always be risky but it is worth noting the consistent themes from the past exercises:

- Few organisations seem to recognise that part of the cost of IT is its security. As desktop computing becomes an everyday part of business life so the need for better security measures will increase.
- Because the cost of computing is falling many more staff are being given computing facilities to perform their daily tasks and yet comparatively few of them are given training in protecting the data on which they rely.
- With so many more users of PCs which are linked to networks, the need to ensure that access is restricted and controlled becomes more important.

As we look to the future, the increasingly popular Internet becomes attractive to organisations anxious to exploit its opportunities for electronic commerce. Whether this will prove to be significantly riskier than other technologies remains to be seen. Telephone systems are also becoming a more popular target for the techno-crook. Perhaps the nature of computer abuse will change with these new applications of technology or we shall see the continued absence of basic controls and safeguards irrespective of technology. Hopefully we shall be able to track such developments through our surveys.

If your organisation has suffered from any form of computer fraud or abuse and you would like to contribute to the survey, please contact the CFS97 Unit in confidence at the Audit Commission, Nicholson House, Lime Kiln Close, Stoke Gifford, Bristol BS12 6SU on 0117 900 1446 or fax 0117 900 1565 or Email churford@district-audit.gov.uk

*Chris Hurford is an Associate Director in District Audit, an agency of the Audit Commission, and he has managed all the previous Computer Fraud & Abuse surveys.*

## Computer Fraud & Abuse Survey 1997

The Audit Commission is undertaking its sixth triennial survey on the incidence of computer fraud and abuse in the public and private sectors of the UK.

The survey will include computer fraud and other IT abuse including hacking, viruses, sabotage, theft of data and software, use of unlicensed software and unauthorised private work. Survey forms are being sent to heads of finance of 5000 public and private sector organisations and the report will be available towards the end of the year.

If your organisation has suffered from any form of computer fraud or abuse and you would like to contribute to the survey, please contact the CFS97 unit in confidence at:

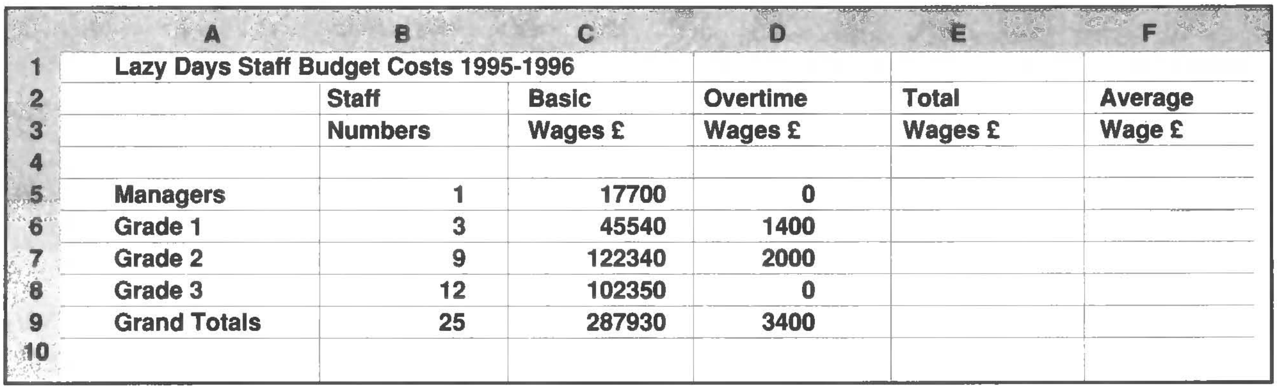
The Audit Commission, Nicholson House, Lime Kiln Close, Stoke Gifford, Bristol BS12 6SU
on 0117 900 1446 or fax 0117 900 1565 or
Email churford@district-audit.gov.uk

# Auditing and the Three A's

**David Chadwick**

Every week my colleagues and I struggle with trying to teach spreadsheets, databases and programming to hundreds of students and to give them some idea of the issues to do with control, audit and quality. It's an uphill struggle but we consider it worthwhile. Year in year out we see students making the same errors over and over again and we try to put them right. Experience has shown that once a student has set-up a spreadsheet they rarely return to look at it in depth again. One wonders, sometimes, if they are mesmerised by the rows of tiny figures which magically change when some key figure is altered. However, as educators, we wonder how they fare when they leave university and start working. We wonder if they still make the same mistakes, repeat mistakes we thought had been cured, or even perhaps invent mistakes never before thought of!

As an example of the kinds of mistakes they make, here is part of a spreadsheet from an actual business (although the real name has been changed). This was given to our first year students and they were asked to enter the appropriate formulae. Perhaps reader, you too would like to have a go and decide for yourself what formulae would be used in columns E and F (the original spreadsheet was in Excel but the actual package is irrelevant).



| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | Lazy Days Staff Budget Costs 1995-1996 | | | | | |
| 2 | | Staff | Basic | Overtime | Total | Average |
| 3 | | Numbers | Wages £ | Wages £ | Wages £ | Wage £ |
| 4 | | | | | | |
| 5 | Managers | 1 | 17700 | 0 | | |
| 6 | Grade 1 | 3 | 45540 | 1400 | | |
| 7 | Grade 2 | 9 | 122340 | 2000 | | |
| 8 | Grade 3 | 12 | 102350 | 0 | | |
| 9 | Grand Totals | 25 | 287930 | 3400 | | |
| 10 | | | | | | |

In the opinion of the lecturing staff the best solutions would be : Total wages in E6 should be =C6+D6 or =SUM(C6.D6) but what about in E5 ? Some students put =C5 but although this gives the correct numerical result surely it is not correct for the underlying model - the user may very well enter another figure in D5 and this would not then be added into the Total.

What about in F6 ? This caused most errors. Over 80% of students entered =AVERAGE(C6.D6). But this gives the average of Basic Wages and Overtime Wages when , given the context, surely it is the `average wage per person' and the formula should be =E6/B6 . On investigation it appeared that students saw the word `Average' in the column heading and immediately applied the average function without questioning whether it was appropriate. This highlighted two very common problem amongst students

- firstly, that of reacting to a `keyword' or `keyphrase' without questioning its true meaning in the given context
- secondly , not really understanding what a built-in function actually did in a practical sense to perform its function.

Although they had successfully used the AVERAGE function before they had failed to understand how it worked i.e. (in Excel) =AVERAGE(B6.F6) would sum the values in the range B6 to F6 and divide this value by the number of cells in the range.

Again, in E9 the correct formula is =SUM(E5.E8) but is the formula in F9 a similar =SUM(F5.F8) ? Over 90% of our students thought so, but if they had really thought about it they would have realised that either the cell should be blank or should contain =E9/B9. Only these two options make sense given the context - to add the average figures together is meaningless.

At Greenwich we have started trying to teach students to `self-audit' their own applications as they go along. We have shown them how to use the built-in auditing features but we found a simpler approach bore more fruit - what we call the 3 A's :Appropriate, Accurate, About-right.

Appropriate : is the formula logically consistent with the underlying business model - eg. this might have prevented the F6 problem above Accurate : is the formula arithmetically correct eg this might have aided prevention of the E5 problem

About-Right : if the incorrect formula of =SUM(F5.F8) had been placed in F9 then 55691 would have been the result (assuming that the average wages were themselves correctly calculated). A student quickly checking would have observed that an average wage for all staff of £55691 could not be correct when the highest paid person, the manager, is only paid £17700.

So far, the 3 A's have helped to give a disciplined approach, leading the students to fully understand the business calculations they are modelling in the spreadsheet. Of course, this imposes a time overhead and it isn't by any means the best solution. There must be easier ways !! This is where we would like to ask the help of all you auditors out there who possibly see errors being made every day.

At the University of Greenwich we are investigating ways of teaching which Try to prevent students making the mistakes that industry claims are being made. Usually academics teach the `right way' of doing something and analyse the ways in which students fail to understand - but, of course, all this takes place in the academic setting itself - not where the skills will eventually be used, in the workplace. This is where we would like to make an appeal to readers of the CASG journal and ask for help. We would like to hear about errors made in spreadsheets and PC- based relational databases where awareness and better training of the user might have prevented the error.

*David Chadwick is a lecturer at Greenwich University*

*Any reader interested in helping David can contact him at:*
*D.R.Chadwick@greenwich.ac.uk or write to David Chadwick,*
*School of Computing & Maths Sciences,University of Greenwich,*
*Wellington Street, London SE18 2PF.*

*The following article was submitted by the partner of a computer auditor. The author has requested anonymity. I can't understand why! - Ed.*

# A View Not From The Back Room

**This is a personal slant on what living with a highly motivated Computer Auditor appears to revolve around. If, by the time you've scanned it and decried it as "the typical little woman's lack of understanding about what's going on", then just let your partner have a look to see if she recognizes the paranoia!**

**Z.Z.Z.Z. -** We don't seem to get a lot of these. It's amazing how," I'm just going to download my mail." stretches into the wee sma' hours. Who does he find to talk to out there? Is the truth out there ? Or is the answer 42 anyway?

**Y. = Yawn** , because of the above AND talk of new, smaller, faster machines that are coming onto the market, but whose price always halves in six months. Well I suppose I wouldn't enjoy a cruise - witches aren't supposed to be able to cross water.

**X. = X-Philes** It's official, it's watched by the professional classes, and it's the only program he will actually come and join me to watch.

**W. = Windows** What can one say ? Maybe Bill Gates is a reincarnation of William Pitt (check out his fiscal policy)- well, the first name is the same.

**V. = Virus** The Medics can't find a cure for them, but he preaches Vigilance.

**U. = Uninterrupted Power Supply** I can't repeat the words used when I thoughtlessly pick up the phone while he's online.

**T. = Telephone lines** No, I am not prepared to have dedicated lines installed, I'm mean!

**S. = Server** Which one to chose? See above.

**R. = Re-boot** I understand when this is necessary that it is a period of great stress and a lot of wandering about the house is called for and a marked increase in the consumption of thick cheese sandwiches occurs whilst waiting for completion.

**Q. = Quality** Whatever happened to hardware/software companies who offered quality and service? I don't know, but I have to censor the remarks about the knowledge and dubious parentage of the poor Sales Staff - we have young children.

**P. = Printer** Yet again I fail to be persuaded that colour printers would be of value to us - I say us, because I am guilty of requesting the odd letter to be printed - anyway, he's colour-blind judging by the creative patterns on some of the ties.

**O. = On Offer** Ah, yes sir, but that piece of software is only on special offer when you purchase the most expensive machine in the shop!

**N. = Norton Utilities** Whatever happened to them ? They fixed everything. Maybe they went the same way as the motorbikes.

**M. = Modem** Run that one by me again. Why do we need a faster one?

**L. = Lap top** What do you mean , "It's obsolete." You've only had it 18 months!

**K. = Kaleidoscope** Yes, I'd pay money to get rid of that screensaver especially that infuriating PING!

**J. = Junior** He is definitely a "microchip" off the old block. He seems to understand the importance of having the nose pressed up against the screen and finger on the mouse for hours on end.

**I. = Icons** I thought these were rather wooden pictures of Russian saints and they certainly need to be looking down here when the installation of some new software is being attempted and it doesn't work.

**H. = Help menu** There's a lost generation out there.

**G. = Games** There will be no games played on this machine. Uh-huh. "They were giving a copy away free."

**F. = Function keys** Must make a note to have some fitted to my spouse. Do they make ones that initiate grass-cutting, fence painting, dog walking or nappy changing?

**E. = Escape** There is none, the lap top goes on holiday too.

**D. = Download** It's like "5 Boys Chocolate" (Ask someone on the wrong side of 40 about it )

AGITATION - someone might've sent something he wants to read

EXPECTATION - someone should've sent something he wants to read

SATISFACTION - someone has sent something he wants to read!

**C. = C.D. ROM** This has been a cunning ploy by the entertainment industry. However, it reminds me of the story about the remote islander who, when he encountered an L.P. for the first time pressed a fork to the grooves and ran as fast as he could in circles to produce some music.

**B. = Baud** An obscure unit of measurement, but surely it was really meant to be baudy - I believe it's very easy to visit these sights.

**A. = Address** Is this going to become a new chat-up line at parties, "Hello, what's your e-mail address?" – I wouldn't know, as he seems to keep changing it . Does this mean the Thought Police are catching up?

# Software Problems?

*We have all come across, at one time or another, those 'undocumented features' that used to be known as bugs. Two of my collegues have found a number of these in a recent release of a product called 'Wife' - Ed.*

Last year a friend of mine upgraded GirlFriend 6.0 to Wife 1.0 and found that it's a memory hog leaving very little system resources for other applications. Hc is only now noticing that Wife 1.0 also is spawning Child Processes which are further consuming valuable resources.

No mention of this particular phenomena was included in the product brochure or the documentation, though other users have informed him that this is to be expected due to the nature of the application. Not only that, Wife 1.0 installs itself such that it is always launched at system initialisation where it can monitor all other system activity.

He's finding that some applications such as PokerNight 10.3, BeerBash 2.5, and PubNight 7.0 are no longer able to run, crashing the system when selected (even though they always worked fine before).

At installation, Wife 1.0 automatically installs undesired Plug-Ins such as MotherInLaw 55.8 and BrotherInLaw Beta release. As a consequence system performance seems to diminish with each passing day.

Some features he'd like to see in the upcoming Wife 2.0:
A "Don't remind me again" button.
A Minimise button.

An install shield feature that allows Wife 2.0 be installed with the option to uninstall at any time without the loss of cache and other system resources.

An option to run the network driver in promiscuous mode which would allow the systems hardware probe feature to have greater use.

His friend responded with. . . . .

I read with interest the article on the WIFE 1.0 product.

I have attempted to avoid these problems by sticking with GIRLFRIEND, but even here I have found problems. I tried installing GIRLFRIEND 2.0 on top of GIRLFRIEND 1.0, but found you must uninstall the older product first, otherwise you get conflicts over the shared use of the I/O Port. Friends have told me this is a long-standing bug I should have been aware of. Anyway, I am now on version 3.0, which, curiously, appears to be an older less well designed version than Versions 1.0 and 2.0, lacking the attractive graphical user interface.

Another problem is that uninstall routine of GIRLFRIEND doesn't work very well as it can leave undesirable traces all over the operating system, and a further annoying feature is that all versions of GIRLFRIEND continually pop up little messages about the benefits of upgrading to WIFE 1.0 A friend of mine tried installing MISTRESS 1.1 on top of WIFE 1.0. He found that WIFE 1.0 deleted the Money files, before it uninstalled itself. Then he found MISTRESS 1.1 would not run, claiming insufficient system resources.

# Outsourcing

*Has now gone to ridiculous lengths as management attempt to abdicate their responsibility for all aspects of the business, apart from the bonuses, as this report shows. - Ed.*

Joe Hacker, Unix System Administrator and father of two girls, has announced plans to outsource his children to a private enterprise specializing in child rearing as part of his family's cost saving effort. Hacker said that his request for proposals will go out later this autumn and that he hopes that a contractor will be in place by Summer 1998.

Hacker says that he anticipates saving 25% of his child rearing expenses by hiring a company which specializes in the field. He believes that between the things that his kids destroy, the wear and tear the kids put on the family residence and vehicles, and the other expenses such as sports, scouts, and lessons, he should be able to pay a private firm about 75% of what he currently spends on his children. Some would say that this approach to family management was adopted 200 years ago in Britain with the arrival of "public" schools.

Although his children have expressed concern that being raised by non-parents would be impersonal and would deprive them of some of their current privileges, Hacker has worked to alleviate their fears. He held a family dinner meeting to announce the decision and told the kids that mere parents don't really know how to raise kids until the kids are grown. This is obvious because every grandparent on the street has advice to give to any parent they meet. A professional child rearing service would already know how to raise children and not make the mistakes of a rookie parent.

The outsource proposal requires companies to provide the children with benefits at at least the same overall level as they receive at home, with some benefits (TV hours for example) expanding, while others (parental attention) declining. The proposal mandates certain "core" benefits, such as food, clothing, and schooling; but, leaves the non-core (music, sports, television) at the discretion of the contractor.

The outsourcing would phase in over a six month period, with the children initially spending daytime hours at their outsource site and sleeping at their parent's home; but, as space becomes available offsite, the children will begin spending all their time away from home except when they are desperately needed at home (for example, when the garden needs "patrolling").

The children originally expressed dismay at residing off-site, but Hacker told them that they would have weekly visitation to the house to retrieve any personal belonging, get new books, 'perform' their musical instruments for, or talk to, their parents. This would also allow the kids to visit their pets (two dogs, three cats), at least until phase 2 of Hacker's cost cutting spree, which includes outsourcing the family pets.

Hacker would not say where he came up with the idea of outsourcing the children, other than to admit that he and his wife were having a discussion about family finances which illustrated the need to raise the family in a "better, faster, cheaper" mode. Although his wife was initially reluctant to have the children raised offsite, Hacker convinced her to accept the scheme because she too was eligible for "outsourcing."

# Hotel and Restaurant Watch

***This is to be the first of what we hope to be a regular feature of the journal edited by Paul Howett.***

**Hilton National, Leeds** - very expensive for a very ordinary room, but does have a swimming pool and sauna . . . .got a phone call in the middle of the night 2.30am that wasn't for me, and newspaper order not carried over to the 2nd day. . . .but did get a free upgrade on next visit when I complained (wow).

**Baros Island Resort (Maldives)** - beautiful luxurious room on stilts over a turquoise sea next to a white sandy beach, swimming from the doorstep and evening baby shark viewing from the terrace....excellent food and (surprisingly) good beer...very informal.

**France: Lille IBIS Centre Ville** approx £30 per night at current exchange rates has its own car park which is very rare and is convenient for all town centre bars and restaurants.

**Aire Sur La Lys** in north west just south of St Omer the Three Mousquatiers hotel approx £60 per night has a very good restaurant. All rooms named after French Dignatories from before the revoloution some have four poster beds !

**Wales: Cardiff Marriot** fine and convenient for centre but a bit pricey, better next door Jurys has a better bar.

**Scotland: Dundee Stakis** fine views of the Tay moderate bar but plenty of choice in the town which is walking distance.

# Letters to the Editor

Dear Editor,

Your editorial in last quarter's CASG journal has stimulated me to write in defense of apathy. When I first thought about your comments, I said I must write. But then I thought, I can't be bothered. Someone else will write. Won't they? And anyway, I wrote a letter a few months ago. Surely I am not expected to write two letters in one year. But as you can see, I decided to write after all.

More seriously, and speaking personally, there are many reasons why the great majority of us do not write and submit for publication papers, articles and so on. Time is one. My family take up a lot of my time and I don't want to sacrifice that for the sake of getting my name in print. I can't write during work hours. For one thing I am too busy and for another as a contractor my benefactor might not see my writing as value for money. And it isn't just the writing. That's the less time-consuming part that comes near the end. There is all that time spent researching your subject. Fear is another. Fear of rejection. Fear that one might not be taken seriously or that one's ideas will be challenged, proved wrong, etc. Perhaps confidence might be a more acceptable term. Talent is another. Not all of us are cut out to write publishable material. Yes, we can all write an audit report but that surely isn't the same thing. Mind you, some of my reports have rivaled War and Peace in length.

Lastly, subject material. Some of us don't have much to say. Even where we do, in our profession, we may breach confidences. So I would like to defend those of us who also serve who stand and watch, (if I may misquote). Without the apathetic, there might be too few readers. If we all tried to write and submit articles, editors like yourself would be overwhelmed and no one would have time to read the articles due to being too busy writing. Oh and there's another reason for not writing, I never know how to finish things like this. I just go on and on and on .........

Yours sincerely,

Martin Welsford

Dear Editor,

I have attended CASG meetings, seminars and technical briefings, whenever possible, over the last 5 years and have invariably found them to be well planned and organised, informative and enjoyable!

Personally, I think the committee has triumphed with the more recent introduction of the technical briefings. The topics have been relevant and the speakers highly competent - you have even managed to deliver any copy handouts promised promptly. All in all, the briefings provide a good opportunity to increase knowledge and skills at a very reasonable cost.

I am aware of the time and effort you have dedicated to the Group over the past few years and I have no doubt that this has contributed greatly to its success. Please, therefore, accept my personal thanks and extend by appreciation to the other members of the committee for the work they do.

Yours sincerely

Anne Elsby
Computer Audit Manager
HM Land Registry
Lincoln's Inn Fields

**Submission Deadlines**

| | |
|---|---|
| Spring Edition | 7th February |
| Summer Edition | 7th May |
| Autumn Edition | 7th August |
| Winter Edition | 7th November |

# BCS MATTERS

Colin Thompson

*__Colin Thompson,__ BCS Marketing Director, outlines some of the current issues for the Society. Requests for further information on these or any other BCS related issues, should be addressed to Colin at The British Computer Society, 1 Sanford St Swindon SN1 1HJ or by e-mail to cthompson@bcs.org.uk*

### Security takes a higher profile

As Society becomes ever more dependent upon computers and computer systems, the need for effective system security becomes increasingly critical. The rapid move towards electronic communication for both business and private purposes over the past few years has underlined that need and there is now a much wider recognition of the importance of security.

Against this background, the Society has launched 3 important new security related initiatives:

- A register of practitioners in IT security
- A new security qualification and the accreditation of courses in IT security
- Creation of a central reference point for information about IT security and audit

### The Register

Organisations need people who are knowledgeable to help them to create secure systems. Security to many people is a black art and those who are new to the subject have difficulty in determining who can help them. To assist in the identification of practitioners with the necessary competence the Society plans to set up a public register of security practitioners. This will be launched later this year and will be open only to BCS members (Professional members and Companions) who have convinced assessors that they are competent in the expertise they profess.

### Accreditation of Courses

The Society has worked with the Confederation of British Industry to develop a guideline for training in IT security. This guideline has formed the basis of a syllabus which has recently been developed by the Society's Information Systems Examinations Board (ISEB). ISEB has also prepared regulations for a national qualification and intends in the near future to invite applications for accreditation of courses. A new qualification in software management, developed in co-operation with FAST is also in plan. Comments on the syllabus and regulations have been invited from the UKISF and other parts of the industry.

### Reference point

The new central reference point which is to be set up within the BCS Web site, is intended to provide a single point of reference for all security related material of interest to practitioners. There is an increasing volume of guidance documents and standards relating to IT security and audit, published by DTI, BSI, ISO, Accounting and Auditing organisations and many others. Some of these are technical, relating to the requirements to permit secure activity at a detailed level, some give guidance to managers in IT and elsewhere in organisations and others provide checklists of desirable controls which should be established over and within IT systems.

Inevitably, in a busy world, it is not always easy to find the particular guidance required and the Society hopes to be able to provide a comprehensive source with an index of the extant material, including documents which are out for comment.

Creating and maintaining a truly comprehensive source will not be an easy task as those involved with the project may not have a complete picture of the available material, particularly where it relates to specialist areas of business. We are therefore seeking help from fellow professional bodies to assemble the material and to keep it up to date so that the reference point is of value to all professionals in the UK whatever their discipline.

This section of our web site (http://www.bcs.org.uk/security.htm) is due to go live within the next few weeks and will contain an Email form by which visitors to the site can notify additional material for inclusion. We hope that this reference point will be a valuable resource for the security community and, if you have an interest in the security field, your contribution will be most welcome.

### Secure Computing

As a further reflection of the importance of security, the Society has established a relationship with the monthly magazine Secure Computing which is published by West Coast Publications. As part of this relationship, all senior BCS members and all members with a professional interest in the security field, are being offered a free subscription.

### A BCS Award for the London Ambulance Service

This year the BCS Management Awards provided evidence, should it be needed, of the benefits of a professional approach to systems development and implementation. There have been few more public failures in the past few years than the implementation of the new London Ambulance Service system. Against that background it was a particular pleasure to see the new team, under the management of BCS member Ian Tighe, receive the 1997 BCS IS Management Award from Sir Michael Heron, Chairman of the Post Office, at a ceremony held at the Roof Gardens Kensington on 14 May. As Geoff Robinson, Chairman of the Judging Panel said in his introduction:

"Ian Tighe and his colleagues have made a major contribution in turning an organisation close to collapse, and the subject of intense public criticism, into one where performance standards are met, morale is restored and the capability to adapt is established. They fundamentally transformed their users' belief in the effectiveness of IT"

### The Year 2000 Publication

The BCS publication *The Year 2000 A Practical Guide For Practitioners and Business Managers* has been a considerable success and we are now on our second reprint. John Ivinson's working has now produced a follow up publication which will be available shortly and is also working on the issue of the single European currency or EMU. Look out for further details of these and other new publications in the computer press and on the BCS Web site.

In the meantime, copies of the first Y2K book are still available from the BCS Marketing Department at £7.50 for BCS Members and £10 for non-members.

**New BCS Training Courses**

As part of the support for practitioners on the Y2K issue, the Society is collaborating with the NCC in delivering a training course entitled The Year 2000 Project Manager's Toolkit. The course is designed to equip those involved with Y2K to scope, assess, plan, monitor and control their projects. Course material includes a comprehensive methodology and the courses are available in Scotland, Manchester, London and in Ireland.

This Y2K course is only one element of a new BCS venture into the provision of training courses. On a wider front the Society recently launched its Professional Development Portfolio, a series of training courses delivered in association with ICL. The initial portfolio focuses mainly on non technical skills in 4 main categories - Consultancy, Business and Finance, Marketing and Selling, and Personal and Communication Skills.

**And Finally ........**

News of another new product available from the Society - the European Computer Driving Licence. ECDL is a European qualification which has been specifically designed for those who wish to demonstrate their competence in the use of IT. ECDL was developed by the Council of European Professional Informatics Societies (CEPIS) with the support of the European Commission and is administered in the UK by the BCS. Copies of the syllabus are available now from the Marketing Department at BCS HQ and it is anticipated that both courses and testing arrangements will be available later in the year.

# Cyber Librarians

## By Hazel Roberts - BCS Librarian

Hello, I am your new BCS librarian having taken over the role from Helen Crawford last year. So I shall be writing regularly for every issue from now on. I expect you would like to know a little bit about myself before I continue. Well, I worked at the Institution of Electrical Engineers back in 1994 as Document Supply Assistant and left in 1995 to become a full-time student, unfortunately that did not work out (being penniless does not agree with me!) so I applied for the BCS Librarian post at the IEE last year and well here I am! I am carrying on with my studying with the Open University,

I am studying Information Technology and Society which is extremely beneficial for this Position. I understand most of the technical computing enquiries which we get from IT experts now! I have to admit my IT knowledge was pretty limited before the course.

**"CYBER LIBRARIANS"**

Many people are unaware of what a Librarian's job actually involves. It is a little more than just stamping books in and out, the jobs are varied and extremely interesting. Most librarians specialise in a particular area. For instance at the IEE/BCS Library we have a total of 14 members of staff who are assigned specific tasks, for instance we have an inter-library loans librarian who can order books or articles from the British Library and she has an assistant who dispatches articles that are in stock in the IEE/BCS library for a charge. Another two librarians look after the journals which are added to our library stock and check to see if there are any new titles available that would be of interest to members.

A Librarian's role has changed over the last few years since the introduction of new Information Technology which has made information more easily accessable and faster to download. Library catalogues can now be searched quicker using a computer database instead of paper filing. By inputting key terms, the computer will tell you what material the library holds on that subject and where you can find it. Librarians today need to have broad information technology knowledge and need constant IT training to keep ahead with new technologies.

The introduction of CD-Roms has meant that information such as a company addresses and phone numbers can be found at the click of a mouse button. Previously searching for information required going over to the directory and thumbing through four or five volumes of that one reference source. Also CD's have meant that paper based directories can be thrown out, which saves a large amount of library space, as the information can be placed onto one disk.

For document supply requests articles can now be ordered on-line instead of by post of fax. This enables requests to be provided quicker. Because of the new technology, Librarians are fast gaining the new title of "Cyber librarians" especially as most information is now found in electronic format instead of paper.

The `Electronic Library' is fast becoming the future. The merger of computing and telecommunications systems has enabled information to become more widely accessable and available to everyone. So, no need to battle for hours in your library trying to locate information that is vital to your company, remember to ask the "Professional Cyber Librarian".

*Hazel can be contacted at the*
*IEE/BCS Library,*
*The Institution of Electrical Engineers,*
*Savoy Place,*
*London, WC2R 0BL.*
*Telephone: 0171 344 5461*
*Fax: 0171 497 3557*
*Email: libdesk@iee.org.uk*

# BCS MATTERS

William List
Chairman of BCS Security Committee

## Security Committee Update

*I am writing to update CASG on the progress of Security Committee initiatives and to ask for volunteers from your group to help us.*

### Register of Security Consultants

The register is on course for a late summer launch. We have decided that the only way to get a discipline procedure in place over persons in the register is to ensure they are members of the Society. A fast track procedure to become members is being put in place.

### Web Site

The security part of the BCS web site will be open soon. This will contain a listing of documents that people active in security and audit should know about and all current documents out for discussion. Once it is ready I will write to you to get publicity for this. We will be asking for help from your members to populate this site with everything they know about.

### Licensing of Trusted Third Parties

A task force has been formed to draft comments for the Society on the governments proposals (available at www.dti.gov.uk/pubs) and to monitor the progress to legislation.

### BS7799 Certification and revision

A task force has been formed to review the documentation expected within the year from BSI and DTI relating to revisions to 7799 and the certification scheme.

The Security Committee would be very pleased if members of the SG could join these task forces. We wish the Society's comments to properly reflect the views of practitioners.

Volunteers should contact me or John Williamson our secretary. The volunteers who came forward in January are being contacted.

# Book Review

| | |
|---|---|
| Title: | **CAATTs and Other Beasts for Auditors** |
| Author: | Dave Coderre |
| Pages: | 238 |
| Price: | £35 IIA Members<br>£45 Non-Members |
| Available Through: | IIA-UK |
| Reviewed by: | Marian Lower -<br>Senior Lecturer South Bank University |

This is not an academic text - not only is it written by an auditor who uses computer assisted audit techniques as part of his routine audit work but it is also extremely readable, jargon free, practical and comprehensively useful. This book fills an enormous void in the market and should appeal to all auditors from the novice to the advanced technical specialist.

The author is very much aware of the need for internal audit to 'add value' to the business, if it is to stay in the business. One way of achieving this is to increase the efficiency and effectiveness of the audit function through the use of technology. His view is that there is a certain inevitability about the future use of Computer Assisted Audit Tools and Techniques (CAATTs) which the modern internal audit function must face up to. He also recognises that the failure to recognise opportunities for the use of automated tools and techniques is the biggest single barrier to the successful implementation of CAATTs. It is in this respect that the book scores most heavily because it contains forty four short case studies describing such opportunities. One example plots the audit methodology from planning to reporting showing how in each phase the auditor can make significant use of CAATTs to improve their efficiency and the overall results of the audit.

The book discusses both the traditional and non-traditional uses of CAATTs. Traditional CAATTs involves the use of basic software like word processing, text search/retrieval, reference libraries and more specialised audit software applications like data access, analysis testing and reporting and standardised extracts and reports. Non-traditional CAATTs embraces value for money auditing, audit involvement in assessing re-engineering activities such as downsizing and bench marking. The audit technology continuum is described at four levels, introductory, moderate, integral or advanced. The introductory stage is basic using automation for primarily administration tasks, the moderate stage is where a few auditors are involved in data extraction, integral where all auditors are involved with the use of CAATTs in all aspects of the audit and advanced where all audit management and auditors are involved with the continuous auditing of key decision support systems. Where are you?

In summary the book covers the:

- definition of audit software tools
- introduction of relevant data processing concepts
- discussion of the implementation and benefits of information technology in auditing
- description of the issues of data access, support to the audit function, and information technology training

The appendices provide some useful information on the Internet and examples of how it can and is being used by auditors. This book should be purchased by every audit function who are serious about developing or using CAATTs - better still buy it for yourself - it will be money well spent.

★ ★ ★ ★ (Highly Recommended)

# Chairman's Annual Report: 1996/97

**Alison Webb**

Thanks to the commitment, enthusiasm and extremely hard work of the committee, we've had a very successful year.

## Membership

Our membership has expanded again, and now stands at around 350, a tribute to our Membership Secretary, Jenny Broadbent. Jenny's phone number is the one everyone is guaranteed to have, so as well as dealing with membership queries, Jenny has been a sort of unofficial agony aunt, sorting out all sorts of members' problems. She is standing down as Membership Secretary (but not from the committee) this year - she really needs to get some audit work done - and she does so with our very grateful thanks.

## Technical Briefings

Our Technical Briefings this year have attracted large numbers, and seem to be providing what we hoped they would: low-cost training coupled with forum to exchange ideas.

Our October Briefing on Audit Automation was organised by Paul Plane and Dave Cox, in conjunction with the ICAEW IT Faculty. It was a very good day, and we have fixed on 27 January 1998 for another joint venture, this time on electronic messaging.

Our January meeting this year, organised by Geoff Wilson and Allan Brown, was also on network security - this seems to be our winter theme. This was at the RAS, and again attracted an audience of over 100.

The burden of administration for numbers of this sort is, as you can imagine, heavy. We decided after January to get some professional help, and called in Jean Brown. She organised the Briefing on 15 April 1997 with Diane Skinner to show her the ropes, and did a terrific job. We hope very much that Jean will continue to help us in the future.

You may also have noticed that there was a bookstall at today's meeting. The IIA produce a range of books specifically on computer audit, and we felt there was much merit in asking them to display them These aren't the sort of publications that are easy to track down in your local Dillons: and they may be just what you need for your next audit.

Apart from the Technical Briefings, Raghu Iyer organised a very successful special meeting on the Millennium and EMU in January. We had a record attendance at an afternoon meeting of nearly 60 for this.

## The Journal

John Mitchell has continued to edit the Journal, and to maintain its high standard. We see this as a very important service to members, particularly those who cannot easily visit London, and I urge people who have ideas to commit them to paper or diskette, and send them to John. Our aim should be mutual aid, and I know many members have experience and expertise they could share.

## Committee

As I said at the start, the success of the group is due to the committee. Apart from those I've mentioned already, John Bevan is our contact with the BSC Security Committee, who are responsible for the Society's official response to public issues like BS7799. He has forged closer links in the past year, and the Security Committee Chairman, Willie List, will be chairing our next Technical Briefing in October.

Geoff Wilson has not only organised a Briefing but is also our representative on the BCS Technical Board. We need to maintain contact with our parent organisation, not least so we can represent the interests of our members, and Geoff has been instrumental doing this. Jennifer Stapleton, the current Technical Board Chair, will be speaking at next April's Technical Briefing.

There will be some changes to the committee next year. Dave Cox has had to resign, because of pressure of work and other commitments. I have always been grateful for the stream of good ideas and useful contacts he has supplied, and I hope very much he will continue to be associated with the group as an active member.

We have two new committee members: Tom Harper, of First National Bank of Chicago, and Mike Demetriou of Lombard North Central, and we welcome them both very warmly.

## Officers

Fortunately for us, our two officers will continue next year. Bill Barton, our Treasurer, has had a very busy year at work, but somehow has still managed to look after our finances with his usual skill and care. His report will appear in the next copy of the Journal.

Raghu Iyer has continued as the group's secretary, and he also organised the special Millennium meeting in January. I find his advice invaluable, and I am very grateful to him.

## Plans for the future

The main item for discussion at the Committee meeting which follows this AGM is our strategy for next year. The Journal and the Technical Briefings will continue: but there are many more things we could and would like to do. The possibilities include closer liaison with other groups, to share what is already available; and more active involvement in public debates. Let us know what you want. And finally, many thanks to all those who've supported and encouraged us over the past year. I hope to see you at many more CASG events in the future.

# Internet-Linked Computers Challenge Data Encryption Standard

*The use of the Internet to harness spare computing power is going to be used by the Search for Extraterrestrial Intelligence (SETI) project in seeking out radio communication from alien intelligences. The potential of harnessing these spare CPU cycles has recently been demonstrated in breaking a DES (Data Encryption Standard) encrypted message. Eat your hearts out GCHQ! - Ed.*

Tens of thousands of computers, all across the U.S. and Canada, linked together via the Internet in an unprecedented co-operative supercomputing effort to decrypt a message encoded with the government-endorsed Data Encryption Standard (DES).

Responding to a challenge, including a prize of $10,000, offered by RSA Data Security, Inc., the DESCHALL effort successfully decoded RSADSI's secret message.

According to Rocke Verser, a contract programmer and consultant who developed the specialised software in his spare time, "Tens of thousands of computers worked co-operatively on the challenge in what is believed to be one of the largest supercomputing efforts ever undertaken outside of government."

Using a technique called "brute-force", computers participating in the challenge simply began trying every possible decryption key. There are over 72 quadrillion keys (72,057,594,037,927,936). At the time the winning key was reported to RSADSI, the DESCHALL effort had searched almost 25% of the total. At its peak over the recent weekend, the DESCHALL effort was testing 7 billion keys per second.

Verser considers this project to be remarkable in two ways:

One. This is the first time anyone has publicly shown that they can read a message encrypted with DES. And this was done with "spare" CPU time, mostly from ordinary PCs, by thousands of users who have never even met each other. U.S. government and industry will have to take a hard look at their cryptographic policies. "DES can no longer be considered secure against a determined adversary", Verser said.

Two. This project demonstrates the kind of supercomputing power that can be harnessed on the Internet using nothing but "spare" CPU time. "Imagine what might be possible using millions of computers connected to the Internet!" Aside from cryptography and other obvious mathematical uses, supercomputers are used in many fields of science. "Perhaps a cure for cancer is lurking on the Internet?", said Verser, "Or perhaps the Internet will become Everyman's supercomputer."

Under current U.S. government export regulations, and underscoring a problem faced by the U.S. software industry, the program that searched the keys could not be exported, except to Canada. A competitive effort, based in Sweden, sprang up well after the DESCHALL effort began. Able to "market" their key-search software around the world, the Swedish effort caught up quickly, and had searched nearly 10 quadrillion keys by the end of the contest.

Verser agrees with the sentiment voiced in RSADSI's secret message: "Strong cryptography makes the world a safer place."

Use of strong cryptography, both domestically and internationally, is essential in today's electronic world. "But not at the expense of a citizen's right to privacy." Verser adds, "Recent proposals for 'key-recovery' and for criminalization of the use of cryptography have no place in a free society."

Information about the DESCHALL effort is available from the official DESCHALL Web site at: <http://www.frii.com/~rcv/deschall.htm

The Data Encryption Standard, DES, is a national standard, adopted in 1977. Use of DES is mandatory in most Federal agencies, except the military. DES is very widely used in the private sector, as well.

Interbank wire transfers, Visa transactions, your medical and financial records, and your employer's financial data are some of the many things secured against prying eyes or against modification by DES.

When the Data Encryption Standard was adopted in 1977, there was some question as to whether or not the Standard was adequate to protect confidential data.

Matt Curtin, Chief Scientist for Megasoft, Inc. says, "This is proving by example, not by mathematical calculation, that DES can be broken with little or no cost." Curtin added, "Others could just as easily be attempting to gain access to multibillion dollar wire transfers."

**Project statistics:**

| | |
|---|---|
| Start of contest: | January 29, 1997 |
| Announcement of DESCHALL project: | February 18, 1997 |
| End of contest: | June 17, 1997 |
| Size of keyspace: | 72,057,594,037,927,936 |
| Keys searched: | 17,731,502,968,143,872 |
| Peak keys/day: | 601,296,394,518,528 |
| Peak keys/second: | 7,000,000,000 (approx) |
| Peak clients/day: | 14,000 (approx, based on IP address) |
| Total clients, since start: | 78,000 (approx, based on IP address) |

**The computer that found the key:**

| | |
|---|---|
| CPU: | Pentium 90 |
| RAM: | 16 megabytes |
| Operating System: | FreeBSD 2.2.1 |
| Speed (keys/second): | 250,000 (approx) |
| Client: | FreeBSD v0.214, built March |
| 12, 1997 | |
| Owner: | iNetZ Corporation,<br>Salt Lake City, Utah |
| Operator: | Michael K. Sanders |

casg
Computer Audit Specialist Group

British
Computer
Society

# Management Committee

| | | | |
|---|---|---|---|
| CHAIRMAN | Alison Webb | Consultant | 01223 461316<br>amwebbcam@aol.com |
| SECRETARY | Raghu Iyer | KPMG | 0171 311 6023<br>raghu.Iyer@kpmg.co.uk |
| TREASURER | Bill Barton | BSkyB | 0171 766 1685<br>bartona@sky.bskyb.com |
| MEMBERSHIP SECRETARY | Jean Brown | | 01803 872775<br>allan.brown@aduk.co.uk |
| JOURNAL EDITOR | John Mitchell | LHS - The Business Control Consultancy | 01707 851454<br>jmitchell@lhs.win-uk.net |
| SECURITY COMMITTEE LIAISON | John Bevan | Audit & Computer Security Services | 01992 582439 |
| TECHNICAL BOARD LIAISON | Geoff Wilson | Consultant | 01962 733049 |
| | Allan Brown | Consultant | 01803 872775<br>alan.brown@aduk.co.uk |
| TECHNICAL BRIEFINGS | Diane Skinner | District Audit | 0117 9001418<br>dskinner@district-audit.gov.uk |
| | Jim Jackson | Lombard North Central plc | 01737 774111<br>jjackson@lombard.co.uk |
| | Paul Plane | National Westminster Bank plc | 0171 726 1882 |
| | Tom Harper | First National Bank of Chicago | 0171 580 8350<br>tharper@fnbc.com |
| | Jenny Broadbent | Cambridgeshire County Council | 01223 317256<br>jenny.broadbent@finance.cambscnty.gov.uk |
| | Mike Demetriou | Lombard North Central | 01737 744111<br>mdemetriou@lombard.co.uk |

Membership Enquiries to:

Jean Brown
26 Rosehill Gardens
Kingkerswell
Newton Abbot
Devon
TQ12 5DN

casg
Computer Audit
Specialist Group

British
Computer
Society

**PLEASE RETURN TO**
Jean Brown
CASG Membership Secretary
26 Rosehill Gardens
Kingkerswell
Newton Abbot
Devon
TQ12 5DN

# Membership Application

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

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

CORPORATE MEMBERSHIP (Up to 5 members)* £75

* Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal *(see over)*

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

INDIVIDUAL MEMBERSHIP *(A members of the BCS)* £15

BCS membership number: ______________________

STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment).

Educational Establishment: ______________________________ £10

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE:
(STD Code/Number/Extension)

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

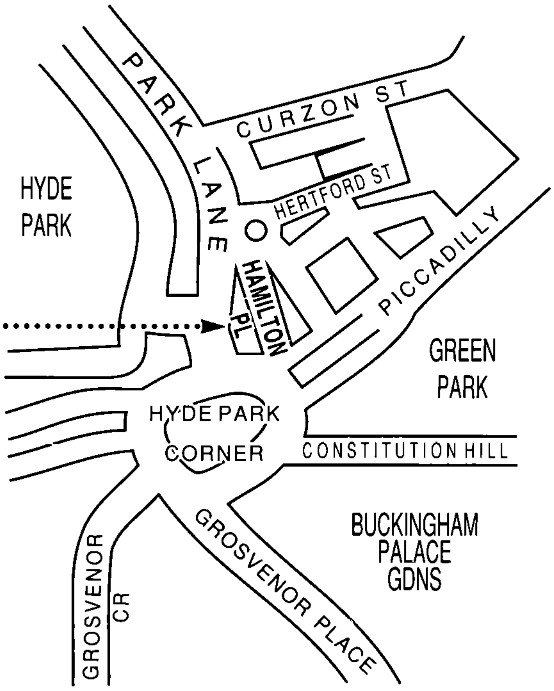
POST CODE:

TELEPHONE: (STD Code/Number/Extension)

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

# Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ


PARK LANE
CURZON ST
HERTFORD ST
HYDE PARK
HAMILTON PL
PICCADILLY
GREEN PARK
HYDE PARK CORNER
CONSTITUTION HILL
BUCKINGHAM PALACE GDNS
GROSVENOR CR
GROSVENOR PLACE