ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 8 NUMBER 3 SPRING 1998

The British Computer Society

Final Technical Briefing for 1997/98 Season

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

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, Computer Crime Consultants
Fraud investigation and internal security	Tom Mulhall, BT

Followed by the Annual General Meeting.

Proposed Programme 1998/99

Technical Briefings

Tuesday 13 October 1998	EMU: Business issue, software issues
Tuesday 26 January 1999	Client/server computing: help-desk, configuration, management, asset management, change management
Tuesday 20 April 1999	Benchmarking IT, Systems development, Data centre

Evening Meetings

Tuesday 1 December 1998	UNIX
Tuesday 16 February 1999	NT security
Tuesday 18 May 1999	Forensic Accounting

Contents of the Journal

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

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

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

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

Submission Deadlines

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

Editorial Panel

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, Berkhamsted, Herts.

EDITORIAL

It is always nice to put together the Spring edition. It means that Winter is almost behind us and we can look forward to those longer, lighter days of the Summer. I took a Winter break in Austria recently, where they have two rates of VAT: ten percent on food and twenty percent on alcohol. The printed till receipt from any sale shows the appropriate breakdown, provides totals of what is being charged at each rate and then shows how much VAT you have been charged in each category. A simple four item transaction produces a till receipt which is over five inches, or 14 centimetres, in length! I am sure that this is all very useful, to someone, and I spent many a happy minute over my food and drink marvelling at this display of information and mentally checking the results.

I came across one where the VAT totals for each category was wrong. For some reason the till could not work out ten and twenty percent with the result that the VAT was being under-recovered by about one percent. This was the only one that I came across where the system was unable to calculate ten and twenty percent respectively, but I wonder what will happen when the Austrian VAT inspectors next visit that establishment? "So mein Herr, you have not collected all the VAT that you should have? You claim it is an embedded processor problem in your till. Have you not read the article by that clever Mr Ashton in the Spring 1998 edition of the CASG *Journal?* No! Ignorance of the problem is no excuse. Even the British are now aware of it and Mr Ashton is both a Kiwi and an Australian, so your excuse is not accepted".

Although Bob's article is written in the context of the Millennium problem, please keep in mind that the EMU will soon be hitting us Europeans and that many companies are now finding that the cost of EMU conformance may be twice as much as that of sorting out the Millennium issue. Does your company have an EMU project underway? If it doesn't, then here is your opportunity to get things moving.

On the subject of moving, a word about the forthcoming AGM. Alison had stated that she will be standing down as Chairman at the AGM. After three years she is allowed time off for good behaviour, but it does mean that we are looking for a replacement. You will find a nomination form in this edition. All the committee places become available for election each year. Why not do your bit, for your Specialist Group?

Hazel Roberts, our cyber librarian at the IEE, has found a fistful of books dealing with security matters and Colin Thompson at the BCS brings us up to date on the various professional registers and the vexed subject of continuing professional development. There is also a useful list of definitions for inclusion in your next audit report. I especially like the definition of 'help'.

Happy reading and I hope to see many of you at the next Technical Briefing and the AGM.

John Mitchell

Chairman's Corner

Alison Webb

When we look at current issues facing computer auditors, one area which is currently receiving a lot of attention is end-user computing. Success here depends in no small measure on how meticulous you are, and this was brought home to me in no uncertain terms recently when I bought a new PC.

I decided to re-install the delivered software, which was NT Workstation. The manufacturer supplied, at a cost, CDs with the code, to save me backing-up first (30+ diskettes - I couldn't face it), and I started quite happily to reformat the hard disk, secure in the knowledge that my supplier was not some backwoods operation in a garage, but a major manufacturer with an excellent reputation for the quality and reliability of its products.

However, they'd added extras to the Microsoft code. These needed to be applied after a patch to standard NT which - you've guessed - didn't come with the CDs. The department supplying the software didn't know that, hadn't heard of the patch and didn't know how to get hold of it - and without it, it was impossible to load a version of NT which worked with their hardware. Just an everyday story of computer folk, after all. However, once I'd tracked down the right extras and got my computer working, I realised that apart from deducing that the patch was missing, all that was needed to make the job simple were four one-line instructions.

Because I have rather a poor memory, I'm quite keen on documentation anyway - but I'm even more convinced now. Fifty words on a bit of paper, and neither I nor the manufacturer's Customer Service Department need have suffered!

We've all had an experience like this, which suggested to the committee that user support in quite a lot of companies could do with some overhauling. A group at CASG are looking at end-user computing at the moment, and we're

hoping to take some initiatives here ourselves. You should hear more about this in the coming year.

Finally, this slot is my last, because I'll be standing down as Chairman of CASG at the end of the season. This isn't because I'm exhausted battling with NT and need time off to convalesce, but because I think that after three years, it's important that someone else has the opportunity to put their ideas into practice. This, then, is my opportunity to thank everyone who's made the last three years so interesting and rewarding.

I've been very lucky during all that time to have been supported by such a good committee, who've worked very hard to organise events and make things run smoothly. I'm especially grateful to Raghu Iyer, our Secretary, and Bill Barton, the Treasurer, who both, despite heavy work commitments, do a great deal for the Group. John Mitchell, too, whom nearly all of you will know from his able editing of our *Journal*, if not otherwise, has been a tower of strength.

We've also had, for the past year or so, Jean Brown to handle our administration, and act on occasion as unofficial counsellor to committee members, especially me, in a last-minute panic about things left undone.

But my final thank-you must be to members, who by supporting our events and contributing to them keep the Group active and enthusiastic. Long may we continue!

Industrial Control Systems and the Year 2000 Crisis

Bob Ashton

This article is intended to bring attention to the potential for disruption throughout industry and commerce which may occur if industrial control systems fail to roll over correctly or cease to function at the start of Year 2000. The article focuses on a description of the problem and suggests ways in which risks may be mitigated.

WHO SHOULD BE CONCERNED

This issue is of particular concern to external auditors who are required to express an opinion of an entity as a going concern. They will be obliged to examine the likelihood of the entity's failure to become Year 2000 compliant within a necessary and acceptable time-frame. Internal auditors who have a duty to alert management of potential threats to their business will also be concerned.

Accounting standards require that if a contingency is expected to result in a loss then an accrual should be included in the entity's accounts at a best estimate.

Compliance officers will need assurance that steps are being taken to ensure that Year 2000 rollover failures will not put their companies in breach of legal requirements.

Banks and other lending institutions will wish to assure themselves that their borrowers will not suddenly cease as viable businesses, thereby liquidating the lenders' assets. Investors will need to assure themselves that they are investing in companies which will remain viable after 1 January 2000. Auditors of such institutions will need to be able to critically appraise compliance statements from borrowers and potential investments. Certain banks and insurance companies have already stated that they will not invest in companies which are not Year 2000 compliant, but lack the means to test compliance claims. These institutions already employ sector analysts whose job it is to provide assurance on the viability of investment opportunities. It is the author's experience that although these individuals may be knowledgeable as to the industry sector in which they specialise, they are substantially unaware of the Year 2000 problem as it affects industrial control systems. Where a level of awareness exists, the assumption is often made that the problem to be solely an Information Systems issue.

This situation may well mean that the auditors of lending and investment institutions will have to perform detailed reviews of the Year 2000 compliance status of companies in which investments are being made.

Credit rating agencies will at some stage appreciate the fact that this issue is also of material consequence to them, as it is of critical importance to the credit rating of any borrower. The Agencies will have to factor in provable Year 2000 compliance into credit indices, thus reducing access to capital and increasing interest charges for companies which are less than fully compliant. Companies which are judged to be bad risks as a result of having made insufficient effort in this direction may well find themselves with no access to credit.

The circumstances of each organisation will be different. It is the task of the auditor, in providing assurance, to apply judgement as to whether plans are in place to at least ensure that vital systems will be Year 2000 compliant, and whether this will be completed in time. It is also well recognised that company directors not exercising due care over company affairs may be held personally liable for losses.

BACKGROUND

Few members of the Auditing Profession will now be unaware of the possible effects of the Year 2000 Problem on computer based systems. Simply put this means that many computer operating systems and applications use only 2 digits to specify the year, rather than 4. Therefore, on 1 January 2000, or sooner for some systems, unless the software is corrected many computers with time sensitive software programs will recognise the year as "00"* or "10"* and may assume that the year is "1900" or "1910" and cause a system shutdown or operate in an unpredictable manner. (* "00" will be recognised in a situation where counters roll from 1998,1999, 2000 - "10" is often returned where only two digits are used 98, 99 and then 100. Because the field size is only two digits the system truncates the last digit leaving "10".)

Many programs calculate the length of time between dates by subtracting 2 digit years from one another. If an application uses the 2 digit date format, it will read the year 2000 as "00" or "10" and be unable to carry out correct date calculations. The application may assume the year is 1900 and return an error message or worse still continue to operate and produce erroneous information. As well as date arithmetic, common operations such as comparing, sorting, and validation can also be affected. These can all result in malfunctions or system shutdowns. This problem is not confined to application programs, but extends to operating systems and firmware.

Any technology which will not correctly process dates after the millennium can be defined as not being Year 2000 compliant. This problem has been well recognised for several years in financial systems which process forward dates and a great deal of effort has already taken place in this area to mitigate the problem. Indeed any one of the Big 6 accountancy firms will be very willing to supply consultancy and tools to remedy the problem in this type of system. However, to date, embedded systems in general, and industrial control systems in particular, have been largely ignored. As a result of this arithmetic errors in embedded systems have a greater potential for causing disruption in the form of significant errors and system shutdowns.

EMBEDDED SYSTEMS

Embedded systems are defined as hardware and software which form a component of some larger system and which is expected to function without human intervention. A typical embedded system consists of a single board microprocessor, with software in Read Only Memory (ROM), also known as firmware. These ROMs frequently start running some special application program as soon as they are turned on and will not stop until turned off (if ever).

An embedded system may include some kind of operating system but often it will be simple enough to be written as a single program.

It will not usually have the normal peripherals such as a keyboard, monitor, serial connection, mass storage, etc. or any kind of user interface software unless these are required by the overall system of which it is a part. Often it must provide a real-time response.[i]

Embedded systems are firmware based devices used to control the operation of equipment, machinery or plant. These include telephone systems, pagers, building maintenance and energy management systems such as heating, ventilation and air conditioning (HVAC), security systems, such as bank vaults, elevators and industrial automation systems that run machinery in manufacturing and processing plants.

Risks

All systems that are date aware are at risk. Some people responsible for these devices in manufacturing and processing plants hold the view that because a device does not need to be date aware, then it cannot be affected by the Year 2000 problem. This is a dangerous fallacy. As standard PC chips, and boards which include Real Time Clocks, have become cheaper they have been designed into in embedded systems, even though theses chips and boards provide more functionality than is often needed. These chips and boards are easily obtained, and with programming modifications, one type can be used in a range of devices. They far less costly than custom chips and boards.

In addition many systems need to be date aware to carry out their function. Some systems maintain the date to determine the day of the week. This is used to distinguish weekdays from weekends. This characteristic is found in systems controlling elevators and building security. Systems such as this are required to behave differently on the weekend from during the week. Other systems measure the time between dates to compute how long it takes to perform some function. Others still, utilise date arithmetic to measure the time elapsed since maintenance checks have been carried out and may fail safe or shut down a system if a pre-determined period has been exceeded.

Practically all laboratory instruments obtainable today depend upon micro chips to function. In many instances, products cannot be shipped until they have been subject to some form of laboratory checking for quality control. All such processes are at risk from failure of these instruments.

The risk exists that if managements do not believe that such devices can be affected, then they will not bother to inventory or investigate them, risking outages and shutdowns which may potentially put their entire businesses in jeopardy.

Further risks arise from the fact that these systems may be in units which are no longer manufactured, or from suppliers who are now out of business, or not able to supply updates for some other reason. In the case of production controllers and monitoring equipment, and safety monitoring equipment, embedded systems can be mission critical. Even if all the systems in a plant are Year 2000 compliant, it is still possible that failure will occur due to communications between devices and systems not being able to function correctly.

Preventative maintenance systems function on calendars to calculate elapsed time for scheduling maintenance work in factory equipment. In some cases where safety is a priority the equipment may be programmed to automatically shut down when the interval between maintenance or calibration checks is exceeded. This can occur when date arithmetic goes wrong and the system thinks that 99 years has elapsed since the last maintenance.

The impact of failure of any these systems can vary from the trivial to the catastrophic.

INDUSTRIAL CONTROL SYSTEMS

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS

These consist of a software application, nowadays generally running on a UNIX, QNX, DOS or Windows platform, although more ancient systems will run on an older generation of computers, such as DEC VAXs, PDP11s or HP 3000s. These systems provide input to, scheduling, monitoring and logging of Programmable Logic Controllers (PLCs) and Field Devices. They usually provide a graphical representation, in real time, of an industrial plant. The display component of the software is constructed using a standard graphics package on a user terminal and provides the user with the ability to affect plant operation from a computer terminal. Custom interface cards in the PC or UNIX computer interface via a data connection to the PLC or Field Device. The data connection protocol utilised will be one of several standards used in industry.

The software application may or may not be Year 2000 compliant. The same applies to the language the application is written in, the hardware utilised and the underlying operating system. The interrelationship between these layers is illustrated by the fact that time stamped alarms at the application level rely on the Real Time Clock (RTC) in the PC at the hardware level to obtain the stamp value.

Risks

Non Year 2000 compliance in the SCADA hardware platform can cause service disruption and failures. Once these systems are in place and working, they do not receive the same kind of attention bestowed on systems found in an IS shop. In particular, there is not the same incentive to keep software releases up to date as this is not the prime concern of the engineers responsible. An operating system upgrade is seen as an unwelcome intrusion into the operations of the plant. Consequently many of these systems will not have been upgraded since they were installed, and may well be deficient in all four areas of application programming, application language, operating system and hardware platform, all of which will require checking. None of these tasks are as straightforward as one might hope. For example, Microsoft, presumably because of their enormous number of customers, will not answer questionnaires on the Year 2000 compliance status of their products. Enquirers are referred to their Web site. Although their pages contain plenty of detail, they require a degree of interpretation on the part of the reader.[ii]

Until very recently, most of the PCs on the market were affected by Year 2000 problems relating to their BIOS and RTC. As PCs controlling industrial plants tend to be older models they will all need to be checked and preferably replaced by up to date models. This will have to be done anyway if an up to date operating system has to be installed in order to support a modern version of the application software or because the old operating system version is not compliant. Besides, the cost of a new PC will be trivial as compared with that of even the slightest plant shut down.

Where Personal Computers used as SCADA platforms are not replaced by up versions, all the following areas need to be checked:

- The Operating System
- I/O Devices
- Real Time Clock
- BIOS
- Network Cards
- Routers

- Other Peripherals
- User Configuration.

An equally long list could no doubt be compiled for alternate platforms.

DISTRIBUTED CONTROL SYSTEMS (DCS)

DCSs are a competing technology with SCADAs and achieve the same results in process control. While SCADAs are generally provided by third party integrators utilising the power of PCs or UNIX computers, DCSs will be sourced from a single supplier promoting a closed proprietary architecture. As an example, Yokogawa, one of the major suppliers, uses standard 3½ inch diskettes to load programs. These cannot be read by a standard PC as their formatting is proprietary.

DCS suppliers generally provide a complete control system for a plant. These consist of modular units containing one or more CPUs of which some will control processes and some support user interfaces. The user displays are similar in appearance to those of SCADAs, except they will be "badge engineered" to conform with the rest of the supplier's products. DCSs interface with Field Devices via a data network. PLCs may or may not be installed in DCS networks between the DCS level and the Field Devices by the DCS supplier, in which case the PLC will be the supplier's own brand. Arrangements will also be found where DCSs talk directly to Field Devices, as sufficient intelligence is provided in the DCS

PROGRAMMABLE LOGIC CONTROLLERS (PLCs)

These are stored program devices which control Field Devices used for process control. They are also known in the U.K as Step Process Controllers (SPCs). The internals of a PLC are not standard as in the PC world, but come from a wide number of different suppliers, each with its own internal design. They will, however consist of a CPU, sometimes with a Real Time Clock, in plug-in modular units. Other modules, of similar appearance, will be input/output units which connect to other PLCs and Field Devices.

PLCs do not have a keyboard or VDU and so do not look like PCs. As little metal boxes with flashing lights they more resemble modem racks. Programming is normally done on a specialist package running on a PC. The language most commonly used is a form of "ladder logic". Each PLC manufacturer will have its own proprietary version of ladder logic. Programs are nowadays downloaded to PLCs in the field by attachment to a laptop PC via its communications port. PLCs will be connected to field devices downstream and may or may not be connected to SCADA systems upstream.

Example of Date Related PLC Failure

At midnight on 31 December 1996, each of the 660 PLCs controlling the potlines at the Tiwai Point Aluminium Smelter in the far south of New Zealand ceased to function. Staff minimised the problems by manually operating the potlines until the problem was fixed the following afternoon. By that stage the damage was done. Without the PLCs to regulate temperatures inside the cells, they overheated and 5 were damaged beyond repair causing $1M of damage. Eastern Australian time is 2 hours behind New Zealand and precisely 2 hours later the same problem occurred at the same company's smelter in Tasmania, a state of Australia.

The control systems for both plants were identical. It was later established that the cause of the problem was that the identical program controlling all 660 PLCs did not take account of the fact that 1996 was a leap year, and it could not handle the 366th day of the year. The Year 2000 is also a leap year, but for reasons stated earlier, the scope exists for many other types of date related errors to occur at this time also.

FIELD DEVICES

These can be divided into Instruments and Control Devices. Field Devices are either connected to a Programmable Logic Controller (PLC) or a Distributed Control System (DCS) by a some form of data network. Instruments are devices used to measure, indicate and record such process variables as flow, pressure, temperature liquid level, pH, conductivity, and product composition and provide information which the PLC or DCS use. Control Devices, such as valve actuators and heaters, receive instructions from the PLC or DCS and change conditions in the plant.

Example of Smart Instrument Failure Risk

It was reported at the Electrical Power Research Institute (EPRI) Embedded Systems Workshop at Scottsdale, Arizona in September 1997: "During a routine shutdown of a 500MW power plant in England, a date roll-over test was conducted on the control system. 20 seconds after the date was changed the plant shut down. The shutdown cause was traced to a "smart" flue stack temperature sensor. The sensor was programmed to integrate and average temperature over a specific time period to minimize fluctuation of the output temperature. The program in the firmware on the chip utilised a real-time clock that depended on the actual date to calculate the time differential."

This is an example of an intelligent instrument being date aware without any apparent need to be. If such an event took place in a blast furnace, then the molten metal would solidify and the brick lining would contract and fall out, leading to millions of dollars of costs in rectification and lost production.

Further Risks

It is likely in many instances that SCADAs, DCSs and PLCs will have been programmed in house. This programming may not be documented and have been carried out by staff who have long since left the organisation. There is no way that the suppliers of these products can provided any assurance that such programming has been carried out to Year 2000 compliant standards.

REMEDIAL ACTION

INVENTORY

An inventory of anything which contains a micro-chip or date dependent equipment will have to be prepared. In view of the limited time left, most organisations will have to conduct this exercise in all areas of their business in parallel. This process will be both difficult and expensive and is likely to require physical inspection of widely distributed hardware and therefore cannot be automated. For most organisations. advice from a central task force will be necessary to ensure that the relevant attributes of each item are inventoried in a consistent manner. It will be necessary to set up a central database of all potentially affected equipment.

RISK ASSESSMENT

This is the determination of the scale of the problem or whether a problem in fact exists. An analysis has to be carried out to establish

the potential impact of the failure of any processes which are supported by items in the inventory. The degree of risk that is inherent in each system or process is then estimated.

The following classification is based on Australian Standard 4360 - Risk Management.[iii]

Level	Descriptor	Example of detail description
1	Insignificant	No injuries, low financial loss
2	Minor	First aid treatment, medium financial loss
3	Moderate	Medical treatment required, high financial loss
4	Major	Extensive injuries, loss of production capability, major financial loss
5	Catastrophic	Death, huge financial loss

TRIAGE

Triage is the process of sorting injured people into groups based on their need for, or likely benefit from immediate medical treatment in a battlefield situation. It is unlikely that companies which have not already made substantial progress into a Year 2000 project will have sufficient time left to get everything addressed before the immovable deadline. In this situation triage will have to be applied so that those items which are mission critical will to be identified and protected first, then areas that are important but not mission critical, and finally the "nice to haves", that can be either worked around if they fail after the deadline or dealt with later.

In order to ensure company survival, a classification such as that described above will have to be used to prioritise systems so that those having risk levels 5,4, and 3 will be addressed in that order.

SUPPLIERS' CONFIRMATION

Suppliers of potentially affected items, initially in the high risk categories, will have to be contacted in order to obtain a statement of the Year 2000 compliance status of their products. As different suppliers may have individual views as to the definition of Year 2000 compliance, they should be asked to comply with a standard definition. Progressive suppliers such as Allen-Bradley[iv] , Foxboro[v] and Schneider have set up Web pages giving this information for their products.

TESTING

Testing should take place for mission critical systems where it is considered that the consequences of failure are such that organisation involved cannot rely on others but needs its own confirmation.

This, however, is fraught with difficulty in the production environment. Testing can only take place during periods of planned shutdown, and even then there is no guarantee that if something fails it will be possible to reinstate it to functioning order. In testimony to the House Subcommittee on Technology, Ann K. Coffou gave an example of tests carried out on programmable thermometers. Of three different models which had their internal dates changed to the century roll over, two stopped working and one could not be restarted.[vii]

Computer software sometimes contain flags which trip after a licence date has been passed. If forward dates are input, these flags may be triggered and the testers may find they are impossible to reset without the aid of the supplier.

If testing does take place, it will be necessary to have a well thought out backup plan so that the system can be reinstated to the status which existed before the test commenced. This reinstatement will need to be performed efficiently and quickly if times-frames are to be met. This will mean having spares on hand for any item which could be affected by the Year 2000 problem. Wherever possible, items should be tested off-line.

Those who doubt the magnitude of this task should consider the following: "As an example of the level of effort required to test embedded logic in a power plant environment, consider this real life Y2K pilot by the Electrical Research Association (ERA) of Great Britain. The boiler control of a National Power (UK) fossil station was reviewed for Y2K impact. This review was limited to inventory, risk assessment and problem identification. All the dependencies were analyzed, both business and system interactions. SCADA interfaces were considered as well. It took a team of 5 people 3 months just to complete the analysis on this single system. This did not include repairs. Scale this to the entire plant. This is what you're up against."[viii]

Readers will be able to extrapolate the time and effort described above to their own industries and organizations, and form their own views as to whether the job is likely to be completed properly in the next one and three quarter years.

RECTIFICATION

Once the above processes have been completed, it will be possible to define the remedial actions appropriate for each system. These will be individual to each situation and could include the replacement of a single chip, software modification or the replacement of an entire system. As this result cannot be known until late into the project, budgeting for such eventualities will be largely based on guesswork.

HEALTHCARE INDUSTRY

The situation in the Healthcare Industry is even more worrying. Hospitals are full of equipment such as PCs, heart defribulators, drug infusers and dialysis machines which provide date stamped logging to enable the physician to monitor the patients condition, and time dependent devices such as drug infusers. All large buildings, including hospitals are heavily dependent on HVAC systems. Failures in patient scheduling could have a very serious effect on those awaiting urgent operations or regular treatment. Public hospitals in particular do not appear to have been provided with the funds necessary to address the problem.

OTHER REFERENCES

Useful information on this subject can be found on the Websites of the Institution of Electrical Engineers[ix] , the Electric Power Research Institute[x] and the Federation of the Electronics Industry[xi]

FOOTNOTE

New Zealand is the nearest industrialised country west of the International Date Line, and so their time is earlier than anyone else's on Earth. During the New Year's Eve festivities of 1999 it will be worth keeping a close eye on what happens in New Zealand in the early hours of January 1 2000. This may give the rest of the world a few hours warning as to whether articles such as this have been heeded.

Bob Ashton CISA CPFA

is currently working on the Year 2000 Taskforce of a major Australian mining and manufacturing group. He has worked in IS auditing and consulting in the UK, New Zealand and Australia in the fields of government, banking, commerce and industry. He is a member of the ISACA Brisbane Chapter.

REFERENCES

i Free On-Line Directory of Computing. http://wfn-shop.princeton.edu

ii Microsoft Year 2000 Web Pages www.microsoft.com/cio/articles/year2000faq.htm

iii Australian/New Zealand Standard Risk Management ISBN 0 7337 0147 7

iv www.ab.com

v www.foxboro.com/prinfo/y2000prod.htm

vi www.modicom/index.html

vii www.house.gov/science/couffou_3-20.html

viii Electric Utilities and Y2K www.euy2k.com/embedded.htm

ix www.iee.org.uk/2000risk

x www.epri.com

xi http://fm6.facility.pipex.com/fei 8 9

Computer Jargon Glossary

(A useful addition to the audit toolbox - Ed)

Alpha. Software undergoes alpha testing as a first step in getting user feedback. Alpha is Latin for "doesn't work".

Beta. Software undergoes beta testing shortly before it's released. Beta is Latin for "still doesn't work".

Computer. Instrument of torture. The first computer was invented by Roger "Duffy" Billingsly, a British scientist. In a plot to overthrow Adolf Hitler, Duffy disguised himself as a German ally and offered his invention as a gift to the surly dictator. The plot worked. On April 8, 1945, Adolf became so enraged at the "Incompatible File Format" error message that he shot himself. The war ended soon after Hitler's death, and Duffy began working for IBM.

CPU. Central propulsion unit. The CPU is the computer's engine. It consists of a hard drive, an interface card and a tiny spinning wheel that's powered by a running rodent - a gerbil if the machine is a 286, a ferret if it's a 386 and a ferret on speed if it's a 486.

Default Directory. Black hole. Default directory is where all files that you need disappear to.

Error message. Terse, baffling remark used by programmers to place blame on users for the programmer's shortcomings.

File. A document that has been saved with an unidentifiable name. It helps to think of a file as something stored in a filing cabinet - except when you try to remove the file, the cabinet gives you an electric shock and tells you the file format is unkown.

Hardware. Collective term for any computer-related object that can be kicked or battered.

Help. The feature that assists in generating more questions. When the help feature is used correctly, users are able to navigate through a series of Help screens and end up where they started from without learning anything.

Input/Output. Information is input from the keyboard as intelligible data and output to the printer as unrecognizable junk.

Interim Release. A programmer's feeble attempt at repentance.

Memory. Of computer components, the most generous in terms of variety, and the skimpiest in terms of quantity.

Printer. A joke in poor taste. A printer consists of three main parts: the case, the jammed paper tray and the blinking red light.

Programmers. Computer avengers. Once members of that group of high school nerds who wore tape on their glasses, played Dungeons and Dragons, and memorized Star Trek episodes; now millionaires who create "user-friendly" software to get revenge on whoever gave them noogies.

Reference Manual. Object that raises the monitor to eye level. Also used to compensate for that short table leg.

Scheduled Release Date. A carefully calculated date determined by estimating the actual shipping date and subtracting six months from it.

User-Friendly. Of or pertaining to any feature, device or concept that makes perfect sense to a programmer.

Users. Collective term for those who stare vacantly at a monitor.

Users are divided into three types; novice, intermediate and expert.

- *Novice Users.* People who are afraid that simply pressing a key might break their computer.

- *Intermediate Users.* People who don't know how to fix their computer after they've just pressed a key that broke it.

- *Expert Users.* People who break other people's computers.

Dick Feynman: Security Guru

Andrew Hawker

Great scientists often come up with ideas which turn out to be useful in ways they never expected. In this respect Richard Feynman, who is best known as a winner of the Nobel Prize for Physics, deserves to be nominated as a founding father of data security.

Feynman's career began when computers were mostly mechanical and did not represent a serious threat to anybody. In 1943 he was assigned to the research team at the Los Alamos laboratories to work on the development of the atomic bomb. It was at this point that he first came into conflict with the Military Mind, which - naturally enough - regarded everyone and everything in the research laboratories as highly secret.

Feynman was fascinated by the security measures imposed by the military, and in particular by the security cabinets in which they kept most of their files. His reminiscences [1] give a loving and detailed account of how he became an expert safe-cracker and code-breaker. In the process he devised techniques which are now discussed routinely in consultants' reports and learned journals. He applied his skills at every opportunity, delighting in the embarrassment of his colleagues when they found that he could raid their supposedly secure filing systems at will.

Initially he found that, nothwithstanding the steel bolts and padlocks on the front of the filing cabinets which everyone was using, the contents could easily be fished out from the back. The management eventually accepted that this was unsatisfactory, and ordered a consignment of Mosler cabinets fitted with combination locks. These Feynman regarded as an even more interesting challenge. His account of the events which followed does not linger on the general reaction of the military, for whom he must have been a quite appalling pain in the neck.

It would not have occurred to Feynman to use his talents in any way which was disloyal, but in all other respects he was an archetypal hacker. He recognised that he needed to do some research into the technicalities of safes, but that this was not enough in itself: and so he proceeded to invent various forms of what we would now call "social engineering". For example he learned how to deduce two of the three digits in a combination code through fiddling with the lock but without looking at it. He would wander into offices, lean nonchalantly on the safe, and hold long conversations about theoretical physics while twiddling the dial behind his back. Having picked off the relevant numbers he added them to a list of all the safes on the site, (which, incidentally, he was careful to keep securely - in a cavity inside the lock of his own safe).

Through judicious use of his list, Feynman was able to create a reputation for himself as a safe-cracker. His policy was to make attempts only where he had already discovered two of the three digits from a previous visit, and he would cultivate the impression that the safe-cracking required much more time and effort than was actually the case. This enabled him to conceal the fact that he only had to hunt for one unknown digit, and kept everyone guessing about his technique. As his fame spread, he found himself being called on to open safes for people who were away from the site (thereby offering the management of Los Alamos what was in effect an unofficial key recovery service). He also found that it could be relatively easy to open safes from first principles. On one occasion, he found helpful clues in the form of a note left in a secretary's desk, and on another occasion he correctly deduced that the key must be based on the date of birth of a daughter of the safe's owner.

Eventually he befriended the official site locksmith (who had, by that time, assumed that Feynman knew more about locks than he did), and the following conversation, full of interesting resonances fifty years on, took place. (The locksmith had just opened a massive safe belonging to an ultra-security-conscious Captain who was away and uncontactable on Bikini atol).

Locksmith: Suppose you had a job as a locksmith and a guy comes down and asks you to drill a safe. What would you do?

Feynman: Well, I'd make a fancy thing of putting my tools together, pick them up and take them to the safe. Then I'd put my drill up against the safe somewhere at random and I'd go vvvvvvvvvvv so I'd save my job.

Locksmith: That's exactly what I was going to do.

Feynman: But you opened it! You must know how to crack safes.

Locksmith: O yeah. I knew that the locks come from the factory set at 25-0-25 or 50-25-50, so I thought, 'Who knows: maybe the guy didn't bother to change the combination,' and the second one worked.

The experiences related by Feynman are salutary not just because many of them have exact parallels with modern data security, but also because of the responses he encountered when he tried to persuade management to introduce more defensive policies. His early campaign to have the original padlocked cabinets replaced was not readily accepted by the establishment. Later, having demonstrated his skills to one colonel, he pointed out that the main source of risk was the widespread habit which people had of leaving safe doors open during working hours. (Feynman needed the safe door to be already open for him to be able to carry out his fiddling-to-find-the-digits routine). The colonel responded by asking staff to try and remember if Feynman had been seen near their safes: if so, they should change the combination immediately. The solution was of course effective, but only in the short term, since staff continued to work with their safe doors open. They had not been made to appreciate the real nature of the risk.

Dick Feynman had a rebellious streak, but he believed passionately in much bigger issues to do with science's place in the world. Given today's technology, he would no doubt have found far more worthwhile things to do than hacking. His understanding of human nature and his love of working with codes (which also made him a source of endless exasperation for the hapless bureaucrats responsible for censoring the mail in and out of Los Alamos) could have made him a security consultant much sought after in today's world.

What Feynman the safe-cracker revealed was that certain things re-appear in different guises, but never really change. It will not be too surprising to find the foibles which he so much enjoyed exposing still in evidence after another fifty years.

Reference:

(1) Richard P Feynman, ed E Hutchings, "Surely you're joking, Mr Feynman", Vintage 1985. A.Hawker 0121 414 6675

A.Hawker@bham.ac.uk Department of Accounting and Finance, University of Birmingham, Birmingham B15 2TT

Information Integrity Research Centre

The Information Integrity Research Centre of the University of Greenwich is a group of academics involved in researching the real-world business problems of preventing, detecting and correcting data and information errors and of investigating better auditing methods and strategies. You may have read articles about their work on spreadsheet errors as reported in the BCS CASG Journal (Summer 1997 edition) and also in the journal 'Internal Auditing' of the Institute of Internal Auditors (May 1997 edition). The spreadsheet work continues but the Centre has extended its research with two new information integrity projects on which it is specifically requesting the help of practising computer auditors:

Project 1:

Investigating strategies for preventing, detecting and correcting Email errors

This project is concerned with the ever-present problems of emails being lost, misdirected or misinterpreted and with the general abuse and misuse of an organisation's email service. This research includes reviewing organisational strategies for preventing, detecting and correcting such problems and for safe-guarding the organisation's legal status with regard to emailed information. The aim of this research is to identify and classify the possible problems that may occur in practice and to review methods of best auditing practice currently in use in business. Ultimately, it is expected to establish and trial an optimal strategy for use by auditors in general.

The project team is interested in hearing from auditors willing to contribute to this research with examples drawn from their business experience. All replies will be treated in confidence. If you would be interested in being involved, please contact:

Philip Clipsham:
email P.Clipsham@gre.ac.uk
phone: 0181 331 8512 fax: 0181 331 8665 or

David Chadwick:
email D.R.Chadwick@gre.ac.uk
phone: 0181 331 8509

Project 2:

Investigating strategies for detecting, correcting and preventing Year 2000 compliance problems in end-user applications (particularly spreadsheets and databases)

The project team is actively involved in performing Year 2000 compliance audits within business. In addition to reviewing their own practical experience, the team are interested in hearing from other auditors on their experiences in this area with the intention of identifying the possible problems that may occur and of reviewing methods of best auditing practice. Ultimately, it is expected to establish and trial an optimal strategy for use by auditors in general.

If you are interested in being involved or would like to know more about what we do then please contact:

David Chadwick:
email D.R.Chadwick@gre.ac.uk
phone: 0181 331 8509 fax: 0181 331 8665

If you would like to know more about the Information Integrity Research Centre, then please refer to our web-site on http://www.gre.ac.uk/~cd02/iirg

Audited into nothing

At Computer Weekly we're used to hearing outrageous claims about the capabilities of IT products. Nut none quite as preposterous as that made by Tally Systems for its Netcensus PC audit software.

Boasting about the success of its product at Birmingham City Council's social services department, Tally claims the software has cut audit times by 1,000%. Given that cutting them by 100% would reduce the audit time to zero, we assume NetCensus can conduct an audit before the council considers doing it. *Computer Weekly*

Student ran porn web site from his bedroom

A student who ran an international porn network from the bedroom of his parents' home has been convicted of publishing obscene images on the Internet.

Scotland Yard's vice squad says it is a landmark result in the fight against global Internet pornography.

It is the first involving anyone from Britain setting up a pornographic website in another country and the first time anyone has been charged with "downloading" obscene images from the Net.

When vice officers raided 20-year-old Timothy Spring's home in Preston they found computer disks containing 5,100 obscene photographs, including hundreds of paedophile images.

Today Preston Crown Court adjourned sentencing of Spring for psychiatric reports.

Spring had earlier pleaded guilty to four charges of publishing obscene articles on the Internet and six counts of making indecent photographs of children.

Evening Standard, 4 February 1998

BCS MATTERS

Colin Thompson
BCS Marketing Director

Colin Thompson, BCS Marketing Director, reviews some of the current BCS news items. Requests for further information on these or any other BCS related issues, should be addressed to Customer Services at The British Computer Society, 1 Sanford St Swindon SN1 1HJ or by e-mail to marketing@hq.bcs.org.uk

BCS Registers

Much activity on the Register front since the last edition of this *Journal*. The Register of Security Practitioners was launched as planned in October and we are currently processing the first batch of applicants. At the time of writing, one candidate has successfully completed the registration process and a number of others are awaiting interview. We are planning to launch the Register to the potential client community in April, to coincide with the planned launch of BS7799 certification - of which more later.

The other new BCS Register, covering BCS members involved in consultancy, has also moved forward over the past few months. Readers may recall that this project started life as a result of a motion to the 1996 AGM from a group of members. A working party under Peter Barnes was set up to consider the proposal and that group produced a 'Green Paper' in April last year. As with the Security Register, Council has always been clear that the Consultancy Register must cover its costs if it is to be implemented, and the task for the last few months has been to establish whether there is sufficient real demand. The results of that exercise represented a considerable success for the advocates of the Register; comments were received from well over 500 members. Most were in support of the plan and over 300 indicated an intention to join. On the basis of that response, Council approved implementation and we are currently planning to launch in May.

I have received queries from a number of members regarding the relationship between the two new registers, and the following brief details might help to clarify:-

Security Register

A fully vetted register. Detailed scrutiny of all applications, including an interview.

Entry qualifications - BCS professional (AMBCS, MBCS or FBCS) or Companion Member with 6 years experience in information systems, 3 years in IS security

Cost - Application Charge £100, Annual Fee £150

Other requirements - two sponsors required

Consultancy Register

To be implemented in two stages. Stage 1 will involve paper vetting but no interview. Stage 2 (after approximately 3 years) will have a scrutiny regime similar to the Security Register.

Entry qualifications (Stage 1) - BCS professional member, involved in consultancy work.

Cost - Annual fee £100

Clearly there will be some members who are eligible to apply for registration on either register. In that situation we would advise entry on both and it is likely that those on the Security Register will be offered a consultancy listing at nominal additional charge.

BS7799

BS7799 - the BSI security standard - is scheduled for wider publicity in April when DTI launches the certification scheme which will enable organisations to seek accreditation of their security processes as BS7799 compliant. The certification work will be carried out by BS7799 auditors and it is likely that BCS will play a significant role in the selection process. The full statement of required attributes for Auditors has yet to be finalised, but we do know that selection will involve both examination and interview and the Society is in discussion with DISC and DTI regarding assistance with both elements.

We also expect the BCS Security Register to play a major part by providing the prime source of recognised 'experts' in BS7799 work. Such experts will be required both to assist organisations with the improvement of their security processes, and to support Auditors as part of a BS7799 audit team. We hope to secure formal recognition of the Register for this purpose and, as part of that, the Society is currently considering whether it wishes to open the Register to suitably qualified non members.

Membership Reviews

BCS membership is currently being examined by two review teams. Mike Allen, the Vice President Professional and Public Affairs, is leading a team looking at ways of simplifying the professional application process. The background to this study is an rising tendency, caused mainly by increasing pressure of work, for applicants to drop out before completing the process. Clearly we need to maintain entry standards with a rigorous scrutiny process, but there is a real need to ensure that the process itself does not impose unnecessary burdens on the individual applicant.

As part of the Review, the team has undertaken extensive research amongst recent applicants and will be running a number of pilot exercises. The first of these, an applicant mentoring pilot, was launched in the Northern Region in February. This will ensure that all new applicants receive a telephone call from a local member within two weeks of application and that contact will be maintained throughout the application process. Mentors will have a maximum of 3 candidates to support and any existing members in the North wishing to volunteer should contact David Parsons, the Regional Officer, by e-mail on parsons@cs.man.ac.uk

The second Review, under Allan Pollard FBCS, is taking a somewhat longer term view of the scope of BCS Membership and considering whether we should retain the existing engineering focus of professional membership or whether we should open it wider to accommodate others involved in the IS field. The emphasis would, of course, continue to be on professional competencies but there is now a wide range of skills involved in delivering IS successfully and not all those involved find it easy to satisfy the existing membership requirements. Allan Pollards team will look at that issue on the basis of the following terms of reference:-

- *to define a proper scope of activity to which professional membership of the BCS ought to be relevant.*
- *To consider how far our current methods of candidate assessment meet the needs of people working within that scope*
- *To ensure that the body of knowledge appropriate to that scope is expressed within the syllabus for the examinations*
- *To align exemption accreditation criteria with that body of knowledge*
- *To consider how the interests of different groups of professional members may be met by a collegiate or faculty structure*

In carrying out the above, to consider how the Society may best serve non professional members

Alan will be producing an initial position paper within the next few weeks which will form the basis for consultation.

Continuing Professional Development

Following a lengthy trial period, the Society has now launched its Continuous Professional Development scheme. CPD schemes are a common feature of most professional bodies and are designed to encourage members to maintain competence by continually updating skills and knowledge.

The scheme now implemented by the Society is a good deal less prescriptive than the pilot system, both in terms of the extent and the type of development activity appropriate. The guidance notes for the scheme recognise that the amount of CPD required will vary from one person to another, depending amongst other things on the demands of particular jobs and the ambitions of the individual. These guidance notes also permit the inclusion of "anything that adds to your personal store of relevant skills, knowledge and experience" whether gained at home, at work or at organised events.

Members are recommended to maintain a record of their CPD on an official record card, which should be returned to BCS Headquarters each January for recording. Those records will be particularly important when members apply for an upgrade in their BCS membership or for Engineering Council registration.

Copies of the guidance notes on the new CPD scheme are available on request.

And Finally .....

News of a radical departure for the Annual General meeting. The 1998 AGM will be held not, as is usual, in London, but in Edinburgh. The Annual dinner, which usually follows the AGM, will stay in London and will be held on a different date. Current plans are to follow the AGM with a lecture.

This move could have something to do with the fact that this years Deputy President, Ian Ritchie, is Edinburgh based, but if the event is successful, we could see the annual meeting being held outside London on a regular basis.

Holiday burglars used airport's computer

A family who masterminded a scheme to burgle the homes of holidaymakers have been jailed after being caught in a police trap.

Southampton Crown Court heard that Katherine Harrison, 23, her father Peter, 46, and brother Gary, 26, all from Totton, Hants, used inside information from an airport computer to set up raids on houses in which thousands of pounds worth of property were stolen. Judge Patrick Hooton said the case represented "just about the worst breach of trust I have ever seen".

The scheme revolved around airport ticket worker Katherine Harrison; all their 22 victims were British Airways passengers. Harrison, who worked for Southampton Handling, a ticket agent for BA, tapped into computer records at Southampton International Airport to obtain passengers' home addresses and the dates of their holidays or business trips.

She then passed the information to her father, who arranged the break-ins with the help of her brother, who carried out some of them.

For six months between October 1996 and March 1997 they used the information to plunder houses across Hampshire. They were only caught when police came suspicious of the high number of the airport's BA passengers being burgled. Detectives sent an undercover officer to the airport, who posed as a wealthy antiques dealer as he made a reservation with Katherine.

The following evening Gary Harrison and a fourth man, Jade Ifould, were caught breaking into the house.

Peter Harrison was jailed for four years for conspiracy to burgle. Katherin received three years for conspiracy and breaking the Data Protection Act. Gary was jailed for six years for conspiracy and burglary, while Ifould, of Lymington, Hants, got two years for burglary and handling stolen goods.

Evening Standard, 7th January 1998

BCS MATTERS

Library Update

Hazel Roberts - BCS Librarian

Happy New Year! Acquisitions in the library over the Christmas period has been rather slow, however now that all the seasonal celebrations are over, the acquisitions librarian here at the Institution of Electrical Engineers/British Computer Society Library is starting to receive more adverts from publishers about new books. Listed below are the most recent additions to our library stock on the subjects of Computer Security, Audit and Internet security. If you are interested in looking at any of these publications or want to find out about any other subjects then you are welcome to visit the library, we are open from 9.00 a.m until 5.00p.m, Monday to Friday. Information about the library services to IEE and BCS Members are available on our web site at: http://www.iee.org.uk/Library/

If you are unable to visit the library and would like to find out what stock the library actually holds, then you can search our on-line library catalogue which can also be found on the library IEE web site. After searching the catalogue and finding a particular book of interest, it is possible for members to order this item on loan by completing a "borrowers" form which is sent by e-mail to the library desk. A librarian will check the details and will send a swift reply. If available, the book will be sent to you by registered post and should arrive within 3-4 working days.

COMPUTER SECURITY

BRITISH COMPUTER SOCIETY
DANIEL. P.
Computer safety, reliability and security, SAFECOMP'97, 16th International Conference proceedings, University of York, 7-10 September 1997.
Springer, 1997.
ISBN: 3-540-76191-8

CARROLL J. M.
Computer Security Butterworth-Heinemann, 1996,
3rd Edition,
ISBN: 0-7506-9600-1

WHITE G.B, FISCH, E.A, POOCH U.W.
Computer System and network security
CRC, 1996
ISBN: 0-8493-7179-1

AUDIT

VAN BIENE-HERSHEY M.
IT Audit handbook, your complete guide to EDP auditing.
Elsevier, 1997
ISBN: 1-85617-275-9

INTERNET SECURITY

PFAFFENBERGER B
Protect your privacy on the internet
Wiley, 1997
ISBN: 0-471-18143-9

MCCARTHY L
Intranet security: stories from the trenches
Prentice Hall, 1998
ISBN: 0-13-894759-7

OPPLIGER R
Internet and intranet security
Artech, 1998
ISBN: 0-89006-829-1

Hazel Roberts -
BCS Librarian,
IEE/BCS Library
Institution of Electrical Engineers,
Savoy Place,
LONDON,WC2R 0BL
Email: hroberts@iee.org.uk
Telephone: +44 (0)171 344 5449
Fax: +44 (0)171 497 3557
World Wide Web: http://www.iee.org.uk/

Russian pleads guilty to internet bank fraud

A Russian computer hacker accused of masterminding the biggest bank heist over the internet - the 1994 theft of $12m (£7.5m) from Citibank - has pleaded guilty in federal court to charges of conspiracy to commit bank, wire and computer fraud.

Vladimir Levin, 30, admitted using passwords and codes stolen from Citicorp customers to carry out illegal transfers from his flat in St Petersburg in 1994.

Money was stolen from Citibank branches around the world and distributed to his accomplices' accounts in Germany, Finland, Switzerland, California, Israel and the Netherlands. Mr Levin, who will be sentenced next month, faces up to five years in prison and a $250,000 fine.

Prosecutors said Mr Levin and five others withdrew only about $400,000 of the £12m illegally transferred. The rest has been returned to Citibank clients.

Mr Levin was held at Brixton prison for over two years as he fought extradition.

Daily Telegraph 27th January 1998

Is there anybody there?

Help is at hand for all those under-resourced and over-worked helpdesk managers. The *New Scientist* has discovered an interesting example of how to provide an optimum service at low cost. New Zealand Internet service Xtra promises customers: "Our helpdesk is available 24-hours, seven days, between 7am and 11pm."

New Scientist

CASG MATTERS

REPORT FROM THE CASH BOX

Bill Barton - Treasurer

The income and expenditure statement includes all Group activities up to the end of our first technical briefing session. This shows a healthy profit to-date of just over £3,000.

Our first technical briefing session, although attracting slightly fewer individuals than the previous year's sessions still resulted in a small profit. We anticipate the joint meeting in January with the Institute of Chartered Accountants will be at least break-even.

On that healthy note, we look forward to a good attendance for the technical briefing session on 28 April 1998, with the subject "Looking beyond the Millennium" to be held at the Royal Aeronautical Society in London W1.

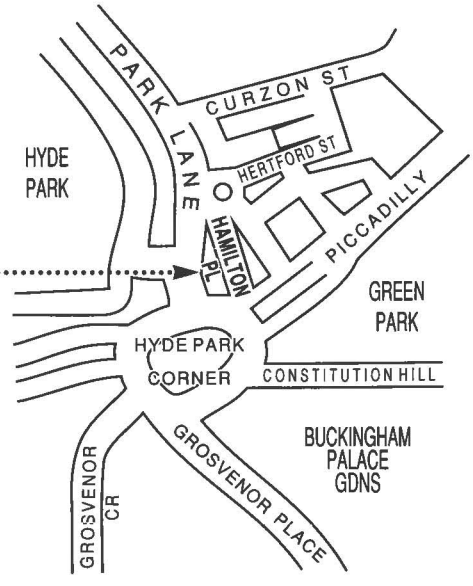
We still have accumulated bank balances of £30,000 from prior years activities. If you have suggestions as to how this money can be used to assist the future of information systems auditing, please contact the BCS - CASG chairperson.

INCOME AND EXPENDITURE ACCOUNT TO 31.12.97

		£	£
Income			
Subscriptions			5,700
First Technical Briefing Session - 15 Oct 1997			3,436
Bank Interest			819
Other:-	ICEAW - Additional Income from 1996/97		
	Technical Briefing	597	
	Journal Advertising	150	
	Recruitment - First Technical Briefing	200	
	AS/400 Book Sale	18	
		965	
			£10,920
Expenditure			
Journal	Summer 1997	1,188	
	Autumn 1997	1,482	
	Winter 1997	1,012	
			3,682
First Technical Briefing Session - 15 Oct 1997			3,148
Administration Expenses			899
			£7,729
Excess of Income over Expenditure			£3,191

Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ



casg
Computer Audit Specialist Group

British Computer Society

Registered Charity No. 292786

THE

ANNUAL GENERAL MEETING

OF THE

COMPUTER AUDIT SPECIALIST GROUP

OF

THE BRITISH COMPUTER SOCIETY

WILL BE HELD AT

4.00 pm, TUESDAY 28th APRIL 1998

AT

THE ROYAL AERONAUTICAL SOCIETY

4 HAMILTON PLACE, LONDON W1V 0BQ

AGENDA

1. Approval of the minutes of the AGM held on 15th April 1997
2. Chairman's Report
3. Treasurer's Report
4. Election of Officers
5. Election of Auditor
6. Appointment of Committee
7. Plans for 1998/99
8. Any Other Business

The meeting will follow the close of the Technical Briefing.
There is no charge for attendance at the AGM which is open to all CASG members irrespective of whether or not they attend the Technical Briefing.

NOMINATIONS FOR THE MANAGEMENT COMMITTEE

As usual at this time, I am asking for nominations for the Group's Management Committee.

We hold about three committee meetings a year, usually at the end of each Technical Briefing. Each committee member is allocated a specific task. The committee is definitely not 'cliquey' and we genuinely welcome new people, new ideas and lots of enthusiasm!

If you would like to discuss any of the committee posts, please contact either Alison Webb (01223 461316), Raghu Iyer (0171 311 6023) or any other committee member (their telephone numbers are given in the *Journal*).

Even if you fancy a post which is already filled, just put yourself forward and the AGM can vote on it. No-one on the Committee will be put out by such a display of interest! A blank nomination form is printed below for your use. Please return completed forms to Raghu Iyer whose address can be found in the Journal.

Remember, this is your group and you should use this opportunity to have your say.

Alison Webb

THE BRITISH COMPUTER SOCIETY
COMPUTER AUDIT SPECIALIST GROUP
NOMINATION FOR THE 1998/99 COMMITTEE

Position: _____

Nominee: _____

Proposer: _____

Seconder: _____

Signature of Nominee agreeing to serve on the Committee _____ **Date** _____

All of the above must be current members of the CASG.

casg
Computer Audit Specialist Group

British Computer Society

Management Committee

CHAIRMAN	Alison Webb	Consultant	01223 461316 amwebbcam@aol.com
SECRETARY	Raghu Iyer	KPMG	0171 311 6023 raghu.iyer@kpmg.co.uk
TREASURER	Bill Barton	Orange plc	0171 766 1600 andrew.barton@orange.co.uk
MEMBERSHIP SECRETARY	Jean Brown		01803 872775 100125.66@compuserve.com
JOURNAL EDITOR	John Mitchell	LHS Business Control	01707 851454 lhs001@aol.com
SECURITY COMMITTEE LIAISON	John Bevan	Audit & Computer Security Services	01992 582439 john.bevan@virgin.net
TECHNICAL BOARD LIAISON	Allan Brown	Consultant	01803 872775 100125.66@compuserve.com
TECHNICAL BRIEFINGS	Diane Skinner	District Audit	0117 9001418 dskinner@district-audit.gov.uk
	Jim Jackson	Lombard North Central plc	01737 774111 jjackson@lombard.co.uk
	David Cox	Lombard North Central plc	01737 776286 dcox@lombard.co.uk
	Paul Plane	National Westminster Bank plc	0171 726 1882
	Tom Harper	First National Bank of Chicago	0171 580 8350 tharper@fnbc.com
	Jenny Broadbent	Cambridgeshire County Council	01223 317256 jenny.broadbent@finance.cambscnty.gov.uk
	Mike Demetriou	Lombard North Central	01737 744111 mdemetriou@lombard.co.uk

Membership Enquiries to:

Jean Brown
Whiddon Lodge
Abbotskerswell
Newton Abbot
Devon
TQ12 5LG

British
Computer
Society

PLEASE RETURN TO
Jean Brown
CASG Membership Secretary
Whiddon Lodge
Abbotskerswell
Newton Abbot
Devon
TQ12 5LG

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 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 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)