ISSN 0961-9348

casg
Computer Audit
Specialist Group

JOURNAL

VOLUME 5 NUMBER 3 SPRING 95

The British
Computer
Society

Members' Meetings for 1995

4 April (4.00 pm for 4.30 pm start)	Joint meeting and debate with ISACA London Chapter **Debate - "This house believes that Computer Auditors are a dying breed and have no place in the auditing world."**	Proposer: Rob Melville City University Business School Seconder: Derek Oliver First Data Corporation Opposer: Charles Mansour, Woolwich Building Society Seconder: Paul Howitt Tesco Stores
10 May (full day) Contact: Jim Ewers 01992 555328	**Discussion Group** Audit & the Internet	See inside back cover for details
10 May (5.00 pm)	**AGM**	See page 14 for details

Provisional Programme for 1995/96 Season
See inside for details.

Meetings are usually held at the Royal Institute of Public Health & Hygiene, 28 Portland Place, London W1N 4DE, except as noted above. For last minute confirmation, telephone the RIPHH (0171-580 2731 or 0171-636 1208). Meetings start at 4.00 for 4.30 pm unless otherwise stated. Tea and coffee are available before each meeting; sandwiches and refreshments afterwards.

Details of discussion groups can be obtained from the relevant organiser.

MAY 1995 DISCUSSION GROUP - SEE INSIDE BACK COVER

IN THIS ISSUE **Secure Systems in the Finance Industry - Refereed Article**

LETTERS TO THE EDITOR

are welcome, write to:
Rob Melville

Centre for Internal Auditing
City University Business School
Frobisher Crescent
Barbican Centre
LONDON EC2Y 8HB
Fax: 0171 477 8880

Editorial

No doubt readers have been transfixed by the disturbing news from Singapore where, depending on who you believe, one of the following disasters occurred:

- a multinational conspiracy against an old established bank
- a council estate barrow boy's street-wisdom failed him and the bank caught a £700 million cold
- even though (unspecified and post event) experts in the business knew Baring's were overextended, nothing was done.

As this journal goes out to people who take a more practical view of these matters, perhaps an alternative scenario can be suggested. Responsibility for this shambles is the fault of:

- management, for not ensuring that internal control systems were set up
- management, for not ensuring that internal control systems were monitored and acted upon
- management, for even thinking that they could put up a false barrier between former Guards officers (senior management, therefore 'innocent') and former comprehensive school dealers and operational managers (lower class and therefore culpable).

Nobody at senior level seemed to complain when derivative trading was bringing in millions the year before. Apart from a bit of false accounting right at the death, the trader in question seemed only to be doing what he was paid to do and earn lots of money with not too many questions asked about how it was done. Only after the event were the obvious questions about segregation of duty and management information asked. My sympathies lie most of all with the auditors, who are on a hiding to nothing here. Either they knew there were potential problems and did nothing, or they did report but not firmly enough.

* * * *

There will be one more journal after which my term as editor will be completed. It's been a tremendously rewarding four years or so and I'm going to miss it like hell. In this time we've moved from a 'house journal' style to a fully professionalised outfit, with excellent typesetting and distribution now outsourced. Editorially we have changed too, with a balance of refereed and practical acticles giving us a useful reputation among advertisers and conference organizers (so you get good discounts). There are almost no bad memories from the last four years, even considering some of the near fatal disasters we've had: like the complete contents of one journal being lost due to a PC failure (no, of course we did not have a back up: we preach, we don't do!) Or the countless times when my office has been full our journals, mail shots and envelopes with a frantic editor trying to make the last post. My sincere thanks are due to my colleagues on your committee who have been unfailingly supportive over the years, to all who contributed, but most of all to Janet our typesetter and distributor and to John Mitchell who between them managed what eight years in the forces, almost as long at college, and too many years at work failed to do and made me meet deadlines on time (well, almost . . .).

ROB MELVILLE

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 action as a result of any view expressed therein.

NEXT DISCUSSION GROUP

SUBJECT: Audit and the Internet

DATE: Wednesday 10th May 1995

VENUE: BCS, 7 Mansfield Mews, London W1

Kings and presidents use it; big business is making its mark; even audit has a presence. Yes, the Internet is becoming really important to us. Here is a chance to get ahead of the pack. Top flight speakers who can speak with authority followed by lively discussion sessions on selected themes.

SPACE LIMITATIONS: As usual we will be restricting the size of the group to twenty members in order to maximise the discussion aspects. Place allocation will be on the usual first booking, first allocated basis so act quickly to reserve your place for this valuable training day.

FURTHER INFORMATION AND BOOKING: Due to the popularity of these events there will be no further notification to you regarding this one, so don't put it to one side to be dealt with later, as you may find that later is too late. Contact the organiser now!

Jim Ewers
Herts County Council
Room 348
County Hall
Hertford
Telephone: 01992 555328
Fax: 01992 555309

Contents

Chairman's Corner

John Mitchell

With all the fallout from Baring's all around us it may be a suitable time to reflect on the role of internal audit in the organisation, but more importantly on our relationship and influence with senior management. Cadbury now requires senior management of listed companies to insert a statement in the annual report on the adequacy of internal control in the organisation. The wording of this was left to the accounting bodies to determine, something which they have singularly failed to do, so it is likely to be a question of 'case law' before suitable wording is derived.

I recently demoaned this to the audience of a conference on the subject and Paul Rutteman, the chairman of the working party created as a result of Cadbury, told me that as the 'Big Six' and the CBI were against the whole thing anyway, there was little hope of consensus on any wording. If Baring's is anything to go by, then I can see the concern of the CBI. It could mean their members facing legal action if they stated that internal control was okay, but they then went down the tubes for £860 million. Poor things! But this is the very reason we need such a statement. It should, and is intended to, make them think twice before adopting cavalier attitudes with other people's money. If they expect to get the rewards, then they should accept the possible downsides as well.

I have been a proponent of risk analysis and control self-assessment for many years. I would have thought that senior management would have leapt at the idea of middle management signing themselves off regarding internal control with the overall process being reviewed by internal audit. Suitable wording, along the 'true and fair' lines would then be a doddle. Everyone gains: the shareholders, because control is actually exercised at middle management and that is where the comfort would come from; senior management, because they would be making a reliable statement; internal audit because we would be spending less time on compliance matters and have more time for educating management in control techniques and getting to grips with value for money. Come along, stick your neck out and go for it. Unless of course you are afraid of explaining to management the concepts of risk and control because you do not actually know what they are.

Guidelines for Potential Authors

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

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

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

Why not call Rob Melville at CUBS (0171 477 8646) to discuss how you can get your name in print?

Business Process Reengineering

Tony Katcharyan
Senior Computer Auditor, The Rank Organisation

On 17th January I attended a Meeting where Peter Adams, an independent consultant who has worked for Digital Equipment Corporation, gave a presentation on Business Process Reengineering (BPR). The following is an expansion of notes which I took during the seminar and which may be of interest to those who were unable to attend.

WHAT IS BPR?

Some key definitions on BPR have been made by Michael Hammer (who with David Champy has written a key book on the subject):

"BPR involves a radical rethinking and fundamental redesign of business processes."

"BPR is a reassessment and realignment of organisations and business processes to fundamentally improve business performance."

The main principles of BPR are:

- Challenge standard operations/processes, question assumptions
- Focus on outcomes, not on tasks
- Think about processes, not functions
- Become customer oriented

In most organisations business functions are vertically aligned (ie there are separate departments for each function), whereas processes which are undertaken are often horizontal in nature and cut through established business functions. The reason for this is mainly historical and originates from the time when division of labour gave rise to the compartmentalisation and the specialisation of predominantly manual functions. Also organisations in the past did not need to adapt to rapidly changing conditions.

BPR is essentially holistic in nature, and focuses on the common area where business methods, technological capability and organisation structures meet. However, the application of BPR within an organisation does not in any way automatically signify success. Failures in the attempt to implement BPR have often come down to a lack of appreciation of human resource problems and organisational issues.

HOW CAN BPR BE USED?

The key issues which need to be considered with BPR are:

- How and where do you start?
- How radical do you want to be? The addition of BPR will have far-reaching consequences the more radical an approach is taken.
- Do you have enough resources/skills/time? How long can a BPR project be expected to continue before benefits must be achieved?
- Which approach is taken - Future Backwards (ie start with the desired goal and work backwards) or Present Forwards (ie start with the present position and work towards the desired goal)?

BPR is essentially positioned at the opposite pole to Total Quality Management, which is concerned with the optimum management of current resources and as such does not encourage radical approaches. Michael Hammer in his literature tends to emphasise the large-scale and dramatic changes which can occur in an organisation through the use of BPR. However, most organisations in practice tend to go for solutions which are around half-way between large-scale and very little change.

The main reasons given for failures when implementing BPR in organisations are:

- Insufficient senior level commitment
- The company was initially not in crisis, and ends up in a worse situation than before
- The BPR team is inappropriate (the team needs dynamic people)
- Unclear business strategy (BPR is no substitute)
- Too much detail examined (often happens with the adoption of the Present Forwards approach)
- Scope of the project is too narrow (ie not horizontal enough, although still needs to be focused)

Information technology now has a significant role to play in the implementation of BPR within organisations. Previously, inhibiting factors which precluded the widespread use of information technology were the cost and inaccessibility of the mainframe computer, the incompatibility of systems and standards, and the cumbersome nature of systems development methodologies. Changes which have allowed information technology to be more widely accepted are the emergence of new technologies (such as workflow software, groupware, graphical user interfaces and networking), client server architecture (which allows the distribution of processes and information), and the adoption of rapid application development and prototyping techniques.

CONTROLS WITH BPR

Controls which need to be considered in connection with BPR are procedural or process controls and system controls. The areas of control are decision points within the process, security, data entry and validation, and audit trails. When considering controls, a trade-off has to be inevitably made between control, flexibility and practicality. The issues which have to be recognised regarding controls when implementing BPR are:

- BPR can radically change the way things are done
- Old procedures which used to work sucessfully may be thrown away unnecessarily
- Processes are streamlined and too many controls may get stripped away
- Management count is reduced, which could affect controls
- BPR focuses externally on the customer, so internal controls may not be given due emphasis
- A less formal and structured approach is adopted for system development
- System development is user-driven, which could lead to insufficient controls and emphasis being placed in certain areas at the expense of the whole.

Despite these concerns, BPR does bring tangible benefits. These are:

- BPR improves the understanding of business processes, particularly the areas of interaction and problem areas
- BPR improves the coordination of activities and the understanding of how the actions of people affect others
- Processes are presented logically to allow the determination of those most appropriate
- Appropriate measurements are installed to monitor processes
- Organisations, processes and systems are more aligned.

Questions which should be asked when considering process controls are:

- How important are controls to the process?
- What are the risks arising from lack of control?
- How can technology be used to build in procedural controls?
- Do redesigned processes conform to legal requirements (eg NHS procurement requirements)?

CONCLUSION

The types of processes where BPR is best adopted are:

- People intensive processes (to cut costs)
- Projects undertaken for customers (eg proposing, estimating, support)
- Where technology can be used to improve the business.

The most common results emanating from the successful use of BPR are:

- Greater support of work from IT systems, such as automatic verification, allocation and routing of work, and communication
- Greater decision-making capability due to people being much closer to the area of work. This should result in an increase in the volume and quality of information, greater responsibility and more authority at the decision-making level
- Close partnership between users and IT departments
- Greater trust in staff
- Greater teamwork
- Increased emphasis on training.

In the future, with the development of products and standards in the transfer of information, many organisations which already work together are expected to work within automated networks. Thus beyond business process reengineering, what is envisaged is business network reengineering, where processes within organsations which work together will be reevaluated. This will involve a focus beyond the single organisation, the creation of information systems to support business networks, and collaborative information systems planning. But the pertinent question to be asked is who will be ultimately responsible for the administration and success of such projects, as they will cut across many organisations?

Despite the above concern it is expected that in future there will be a greater dependency on computer systems and fewer administrative staff will be required within organisations. It should also be noted that IT departments are expected to decrease in size with fewer permanent staff and a greater proportion of contract staff.

The question of how BPR can be adopted within the audit process is more difficult to determine. It is probable that more audit functions will be automated with the use of groupware and intelligent flowcharting software. One final thought for auditors whenever they consider the use of controls within business processes: it may sometimes be preferable to give up certain elements of control in order to gain more overall control within the whole process. ■

Portable PC's - productive tools and potential disasters?

John D Bevan

The author

John Bevan has been working as an independent consultant since 1989, trading as "Audit & Computer Security Services", carrying out assignments, providing consultancy advice, developing and delivering training in computer audit, in computer security, and in other specialist IS areas. Most of his work is done in the UK, and much away from his Hertford office. This article describes the author's recent mixed experience of updating his own portable computing tools.

Seduction

I have seen the portable PC adverts. With a portable I can work eighteen hours a day: in the office, at home, on the beach, and when travelling between them. It will improve my productivity, and my image! I shall no longer have to share a PC in clients' offices with permanent or other nomadic workers. I shall not have to switch between Mac's and PC's, between UK, US, Turkish, and Arabic keyboards, between DOS and Windows, and between different word processing, flowcharting, spreadsheet, and other packages. Being self-sufficient and familiar with my own portable PC, and with its installed software, I know I can work faster, longer, and to earlier but realistic deadlines. This is a competitive necessity.

Although a portable hard disk would allow me to carry my own data and software with me, and is cheaper, it requires that a PC be available whenever needed, and may offer only moderate performance. Some inexpensive portable computers (such as the Cambridge Z88 or Psion MC400) provide good word processing functionality and a long battery life, but do not run Windows software, and so are unsuitable.

With 486 processors, local bus graphics, and large hard disks, portables are now more powerful than my old desktop 386. I can probably sell the 386 and buy a 15-inch SVGA monitor to plug into the portable, and use them together as a desktop. The PC magazines describe many portables, with well-known brand names and from smaller suppliers. The reviews seem to say that you do not need to choose a well-known brand for good performance and design. It's the other suppliers whose products are often assessed as giving the best value for money, and sometimes the best performance. Magazine tests suggest that, on the move, a powerful portable's battery life is typically up to 5 or 6 hours. So, after trying demonstration machines, I order a well-reviewed product, not a well-known brand, from a local (BS 5750 certified) supplier, whose premises are well equipped and staffed with pleasant, technically knowledgeable people. I receive in writing a personal price quotation and detailed specification, with a monochrome screen, DX266 processor and a minimum on-the-move battery life of two to three hours. My current contract takes me to and from Scotland each week by train, during which I shall often use the portable's battery.

Disappointment

A few weeks later the portable arrives by carrier, with DOS and Windows already installed. I read the manual (I've worked with computers for many years), and install my favourite Windows word processing package. In use battery life varies from ten minutes to an hour and a half! The manual promises four to five hours. What am I doing wrong? I re-read the manual, find a few mentions of APM (something power management), but still cannot find out whether it is installed or not. I check my observations, then phone the supplier's Technical Support. I am gently told that I am being too optimistic about battery life, and that in this competitive market many suppliers imply (but do not guarantee) that their products will run on batteries for much longer than they will in practice. Some power saving suggestions are made, which I adopt. Only marginal improvements materialise. I call again, when it is discovered that through some oversight by the supplier the APM/battery icon in Windows is missing. The supplier faxes me detailed instructions, and I re-install DOS and Windows, taking a few happy hours. The APM/battery icon appears! I am also sent another battery pack. Battery life now approaches, but does not reach, two hours. At my suggestion the supplier investigates fitting a lower speed and lower voltage processor chip.

Sympathy

I call three friends with portables who also work in many different offices. The portable Mac user is well satisfied - his new machine's battery lasts for two to three hours. The second says she rarely uses the battery, but that I should not buy the brand she has as it has gone to be repaired yet again. The third friend is in a similar position: after a time-wasting dispute with the supplier his newer machine is being repaired under guarantee. His experience of battery life is up to two hours. He tells me a story of a client who writes off the value of company portables over eighteen months because few last much longer!

Betrayal

I have been tolerating the occasional failure of the portable's left trackerball button. It can be fixed when the processor is changed. I have learnt to use the machine's rapid suspend-to-disk/resume facility to save work done. After spending an hour writing a report on a train one evening, it takes many attempts to get the suspend button to activate suspension. Now disaster strikes! I cannot then power on the machine. I leave it on the charger overnight and go to bed. Next day all I can think to do is to remove and refit the battery pack. I can now power on, but all hard disk records of my report have gone. I wish I had not turned off the word processor's auto-save function in order to reduce battery power consumption.

Divorce

I call the supplier and tell him firmly that I have had enough. After almost two months the battery life problem has not been solved. To my relief, and somewhat to his credit, he agrees to a refund. I still have to pay for delivery by carrier and for opening the DOS and Windows packs in order to re-install these! I protest that this is unreasonable, but without much conviction. The experience has cost me about £100 and many hours of my time, but I am a little wiser. What have I learned?

Reaction

For two months I have been carrying around an insured notebook PC with a spare battery and power supply, together weighing more than the quoted weight for the portable - so I want a lighter subnotebook (with a footprint smaller than an A4 page) with a small power supply. However I am not willing to forego a floppy disk drive, as I am going to use this to back up my new or changed files every hour or so in future! I know that a fast processor chip will consume more battery power, so I shall be satisfied with a low voltage SX25 or SX33 processor. I want reliability, but do not really know how to find it. I guess that well-known brands are more likely to supply it. I am lucky, and buy a nice machine, which satisfies these revised needs, without having to pay much more than I paid for the first machine. I have been using it successfully for three weeks now.

Conclusion

Portable PC's can deliver many of the benefits claimed for them. However they can be a real pain in the neck, sometimes quite literally. Many, when packed in a bag with a power supply, cables, spare battery, and mouse, can weigh almost as much as many of our briefcases. They are expensive, often contain much confidential information, and being portable are easily stolen. They should be properly insured and cannot be left just anywhere. This means either locking them away when you go home from the office or go to lunch, or taking them with you! A bag obviously containing a portable PC also makes its owner an attractive target for muggers, especially in some areas late at night. I am told that two people carrying portables were recently mugged near an office I was at last week. You decide whether to take body building and self-defence classes!

Most portables seem to me to be less reliable than desktops. It is difficult to quantify this. I have already given you my own impressions. Figures from PC Magazine (August 1994) tend to support my view, although its reliability survey findings are restricted to relatively well-known brands. Its regular reviews of new portables are more extensive than most, but make no comment on reliability. Again this magazine goes further than most in attempting to measure and assess battery life, but in my experience still stimulates over-optimistic expectations. When a portable PC fails, it is often slower and more difficult to mend than a desktop. If my old 386 fails, I can quickly and easily remove the defective unit and replace it with another, relatively cheap, and standard, unit (disk drive, motherboard, keyboard, etc.). Portables are different: they are more difficult to open for repair, and component sub-assemblies are often proprietary, with replacements less readily available and more expensive. Take IDE hard disks, for example. They are usually smaller and more expensive than those supplied in desktops, and take their power supply through the multi-way interface connector, rather than through a separate power connector as on a typical desktop. Thus it is more difficult to remove an IDE drive from a failed portable, install it in a desktop PC, and recover its data. This requires more technical ability and resources than for a failed desktop.

It is clear to me that it is more important to protect data on a portable against the effects of possible failure, accidental loss, and theft. For me more frequent back-ups to diskette are the answer. Do not buy a portable without a diskette drive! These considerations also suggest that you keep your desktop machine, secure and use the same software on both portable and desktop. If the portable fails or is stolen you can at least continue to work on the desktop.

The mobility of the portable and of its owner also increase the risks of the disclosure of confidential information and of virus infection. Get a portable with a BIOS level password and use it, install and regularly update virus protection software, and consider software that encrypts particularly sensitive files. Anti-virus products should be well known by now. Utility packages (e.g. PC Tools), public domain software (e.g. IRIS), and security software (e.g. PC Guard) provide suitable encryption.

Most of these conclusions still apply to those of you who work for large organisations. However for you it may be easier and as effective to back up your portable's new and changed data to network drives at docking stations, provided these are found wherever you work. A few spare portables can cover the risk of single portable failure, instead of using desktop PC's as is suggested above. ■

Abstract

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

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

(Part 1 of 3)

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

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

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

1. Summary

Background

In his book 'Management Strategies for Information Technology', Michael Earl makes the point that as the field of information management has matured from the early ad-hoc days of data processing to the more rigorous era of information technology, management has stopped viewing computer systems as a cost and started seeing them as an investment. A similar transformation is taking place in the security industry: attitudes are changing as the field matures, and computer security is starting to be viewed as an investment rather than a necessary evil.

This change in the financial attitude towards security is just one of the differences of approach between the two eras. The main distinctors are in figure 1.1. Together, these changes signal a radical shift in the way companies must tackle security. In financial terms, instead of minimising the cost of security, they must now maximise the return on their investment. To be proactive rather than reactive, they must be able to forecast in advance what threats will be encountered. To combine four separate types of countermeasures (see figure 1.1.) into a coherent whole, security must become the responsibility of every department, not just the IT department.

Figure 1.1. Two eras of computer security

Distinctor	**Immature Stage**	**Developed Stage**
Financial attitude	A cost	An investment
Technologies involved	Computing	Computing, Personnel, Procedural, Physical
Employee Awareness	Low	High
Management Responsibility	IT Department	Company Directorate
Stakeholders	Few	All users
Motivator	In response to discovered threats (reactive)	In response to forecast threats (proactive)
Development Stage	Added on to existing system	Part of system development
Type of countermeasures	Stand-alone	Integrated

Security is maturing as a matter of necessity, not as a result of natural evolution. Computer crime has been identified as a serious threat and as a growing threat. The NCC Survey 1991 calculated the annual cost to British industry from security breaches to be £1.1 billion. Furthermore, this cost is only the immediate costs of detecting and repairing and/or rectifying the breach: it does not include long-term costs such as loss of business, damage to reputation, etc. The Home Office estimated that credit and debit card fraud added a further £165m to this total in 1991 (Financial Times, 09/07/92). No more recent figures were available at the time of writing[1], but reports from a number of more sector-specific bodies indicate that crime is increasing. CERT[2] have warned that 'break-ins on the Internet are growing at an alarming rate (Computing, 07/04/94). The Commission of the European Communities has stated that there is a 'growing dependency' on distributed systems and a concomitant need to improve security (INFOSEC Call for Proposals Work Plan '93, 03/08/92). Paul Shapira of ICL Secure Systems states that, in the non-military sector, 'the overall need for security is now growing' (1992, p5). Cranny, '88, notes that 'computer based fraud can be seen as one of the fastest growing industries of the 20th Century'.

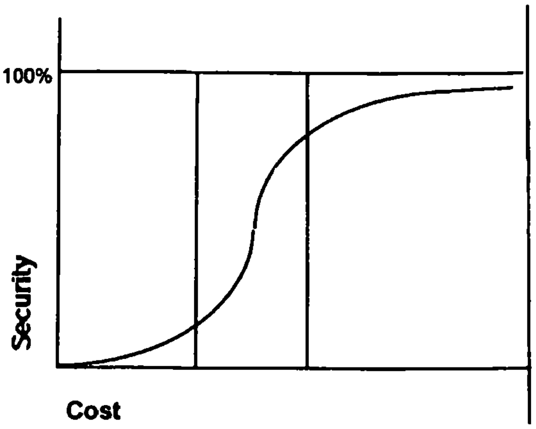
Shapira, also notes the change in development stage and type of countermeasures described above: *'Until about the last two years, commercial and other non-military organisations have demanded little security of the IT industry other than the need to counter severe threats in an ad hoc manner as they become apparent and critical'* (1992, p5).

Alderton (1990, p2) supports the changing financial view of security by noting that companies are changing the basis of their financial justification for security. The usual financial management approach to spending money is to minimise costs and maximise return on investment. So, as security changes from a cost to an investment, the whole practice of cost-justification for security changes. Minimising the cost of security leads to developing the least expensive security countermeasure that will solve the current problem. The 'security as investment' view leads to maximising the return on the investment, and realising that security is not a binary function.

Alderton (1990, p6) measures the 'level' of security against the cost as an asymptotic S-curve (see Figure 1.2.). At first, minimal security is achieved for very little expenditure. There is a rapid improvement in security for little increase in expenditure in the middle region of the curve. After this, the curve indicates a diminishing return for increased expenditure, but never reaches the '100% secure' mark.

The curve never reaches 100% because there is no such object as an entirely secure computer system. There are three main reasons for this, which apply to almost every security countermeasure in some form.

Figure 1.2. The cost of security



- Countermeasures can be bypassed or broken given sufficient time and resources.
- Security threats are constantly changing in unforeseen ways.
- Countermeasures depend to a great extent on system users.

These three points will be expanded on in sections 2 and 3, in relation to particular threats and countermeasures.

Introduction

The background provides all the supporting arguments for the hypothesis: namely that a holistic approach to security countermeasures is more efficient than stand-alone measures.

A holistic approach can be defined to be an*integrated policy of security countermeasures, comprising quantification measures, personnel and procedural measures, deterrence measures, defence mechanisms and minimisation measures, composed so that the measures complement and overlap each other.* This runs counter to the industry norm, the specialised approach, whereby countermeasures are taken from one or two only of the above listed five types.

This reason this approach is more efficient than the specialised approach is due mainly to Alderton's S-curve. After a certain threshold, the cost of security increases out of all proportion to the increase in security functionality. Only in exceptional circumstances will it be worthwhile purchasing security measures above this threshold. The return only justifies the expense when protecting against an extremely high-risk threat. Instead, it is much cheaper to purchase two security measures

[1] New surveys by NCC & Audit Commission were issued in 1994, showing broadly similar figures.

[2] The Computer Emergency Response Team, an industry body created to monitor Internet security.

from within the centre region of the curve, where return on investment increases significantly with minor increases in investment. If these two measures are chosen carefully so that they overlap and support each other, a high level of security is achieved from two measures at a cost less than that of a comparable single measure.

The Five Shields Model

The Five Shields model has been developed by the author to aid in designing a holistic security policy. It is a graphical model to aid in assessing system vulnerabilities and appropriate responses to particular sets of threats. The model is wholly qualitative, and is designed to complement, rather than replace, quantitative methods such as risk analysis (q.v.) and Burch and Grudnitskis (1989) Optimum Mix of Controls methodology. It is fully described in section 5.

The model is validated by applying it to the case study company, Chelsea Ltd. (q.v. 1.5., Appendix A), a London Stockbroking firm. It clearly shows the main vulnerabilities in Chelsea's computer security, and generates simple recommendations as to how to radically improve security at relatively little expense.

Methodology

The essential argument in favour of the holistic approach can be broken into two parts: firstly, that individual threats cannot efficiently be combated by individual countermeasures; and secondly, that countermeasures from different areas support and enhance each other. Therefore the supporting argument can be split into two parts. Firstly, in section 2, a brief description of the main threats to systems security is essayed, and for each threat, the difficulties of successful prevention by stand-alone measures is explained. Section 3 contains an explanation of further 'complicating' factors, which prevent stand-alone countermeasures from operating at full effectiveness.

Secondly, in section 4, an outline of the major security countermeasures is presented, along with a discussion of how they are limited when implemented alone, and how they can complement and support each other.

Section 5 describes the Five Shields model.

Section 6 contains conclusions.

The argument for the holistic approach was set against the background of the financial sector because, although the risks faced by financial institutions are very similar to those faced by any other organisation with large scale data processing systems, the level of exposure in the financial sector is much greater. This is due in part to the lack of awareness of computer security among staff in such institutions: according to Sherman (1991), *"There is ample evidence, from a number of widely publicised and reputable surveys, that even some of the largest and most well-established banks - let alone smaller banks - have yet to establish comprehensive levels of security in their electronic banking networks"*. The banks have greater exposure, but less existing reliance upon any particular approach, and form a more open field for investigation.

Case Study

During the course of this paper, extensive reference is made to a case study of a small city stockbroking firm, to better explain or support points raised in the text. It is also used to illustrate how various countermeasures could be implemented, and to discuss the effect they would have on the organisation.

However, the main purpose of the case study is to provide a validation of the Five Shields model. The model is applied to the study in section 4 to analyse the vulnerabilities inherent in the case study's security measures, and present recommendations for improvement.

The firm was selected because it has a very low level of security protection, and typically serious consequences of security breaches. The problems faced by this company are considered to be representative of those faced by most financial organisations, of any size.

The company is a registered stockbroker in the City of London, but, for reasons of confidentiality, does not wish its name published. Therefore the name of the company has been changed to Chelsea Ltd. From time to time, reference is made to possible security breaches and incidents involving Chelsea Ltd. It must be stressed that these are purely hypothetical situations, and are not reports of actual incidents.

Chelsea Ltd operate in the same way as do most stockbrokers. Their operations are divided into two sections, known as the 'front office' and the 'back office'. The front office consists of the brokers themselves, and the back office the necessary support staff. As far as the brokers are concerned, accurate information and speed of operations are by far the two most important factors when it comes to making money, and anything that slows down the trading process should be avoided at all cost.

It is not surprising, therefore, that the company has an extremely poor culture of security. Their security procedures are minimal and rarely policed, and the IT manager, ultimately responsible for all systems security, does not believe that there is any point in attempting to secure systems.

As ever, the effects of a possible security breach at the company range from the petty to the paralysing. In the worst case scenario, a fraudster could transfer millions of pounds into an overseas bank account via the company's electronic fund transfer system. This could do irreparable damage to the company's reputation, prestige, and balance sheet.

The above are the main points of the case study. Appendix A offers a fuller description of Chelsea Ltd.'s IT systems and security measures.

2. Major System Vulnerabilities

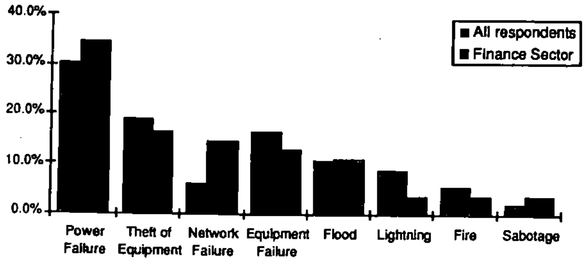
This section offers a brief overview of the main threats to any IT system. These definitions are intended as a guide only, and references are provided in case a more detailed examination is required.

Physical Threats and Denial of Service

Physical threats to computer systems accounted for slightly over half of the total NCC estimate of costs of security breaches. Most physical breaches cause a denial of service, and so the two categories can be considered together.

Denial of service occurs when a computer system fails to provide the service for which it is designed. This can occur for a wide variety of reasons, ranging from: loss of power to the system; unexpected hardware or software failures, or 'crashes'; deliberate denial of service due to hacker attack; vandalism or theft of physical computer resources; a system overloaded with too many processes, often caused by rogue programs or natural disasters such as fire, flood or lightning. The only other physical threat noted by the NCC Survey was that of direct vehicle impact on hardware, suffered by only 1% of respondents.

Figure 2.1 Physical Breaches by Type



Source: NCC Survey 1991

Physical threats are largely self-explanatory, and as such no further references are given.

Figure 2.1. shows a breakdown of physical breaches by type within the finance sector. Figure 2.3. (q.v.) shows a similar breakdown for logical breaches. However it should be noted that these graphs merely display the number of reported breaches of each type, and do not reflect on the cost or severity of the individual incidents.

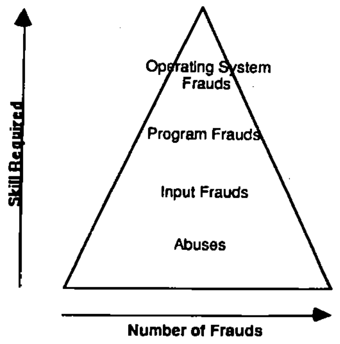
Fraud and Direct Theft

Fraud can take a wide variety of forms, from credit and debit card fraud, through loan fraud, investment fraud, accounting fraud and cheque fraud. An increasing amount of these frauds are being carried out through information systems. An indication of the reasons behind this can be gained from the average return on various types of fraud. The average return from an armed bank robbery is $4,000; the average return from a paper-based fraud is $30,000; and computer-based frauds average over $600,000 (Burch & Grudnitski, 1989).

The most widespread form of IT fraud is credit card fraud and debit card fraud. Estimated to have cost between £165m[3] and £400m[4] in 1991, credit and debit card fraud is becoming a major problem for banks. However, credit card transactions in Britain in 1991 amounted to £29.35bn, and debit card transactions amounted to a further £9.51bn. Therefore APACS' estimate of £165m represents only 0.25% by value of all transactions. This does not appear to constitute a great problem, but banks are working on a merchant service charge of 2-4%, so this represents between 6% and 12.5% of the banks' revenue. The major banks collectively pledged £500m in 1991 to technology-based solutions over a 3-5 year time scale. The benefits from this investment are beginning to show as a reduction in the level of 'plastic' fraud in 1994.[5]

The number of frauds committed varies according to the skills available. Figure 2.2. shows the 'fraud pyramid' of number of cases committed against skill level needed. Simple abuses of a system, which form the major part of credit card fraud, each cost relatively little, but the sheer number of offences causes the total cost to increase.

Figure 2.2 Fraud Opportunities Pyramid



Source: 'What Price Security', A.D.D. Alderton

[3] Estimate by the Association of Payment Clearing Services.

[4] Estimate by Central Cheque Squad, New Scotland Yard.

[5] These estimated costs are not included in the NCC survey estimate of the annual cost of security breaches.

Fraud has always been big business, and computer fraud is no exception. On of the largest ever corporate frauds, against Equity Life in Los Angeles and worth approximately £220m, was committed using their information systems (Burch & Grudnitski, 1989). Elaine Borg, a programmer at the Henderson Group, a UK investment giant, was recently convicted of attempting to embezzle £15m from Henderson's Digital-based systems (Computing, 25/03/93). In 1987, an attempted fraud of $8.5m at Prudential-Bache, New York, was discovered and stopped at the eleventh hour (Investors Chronicle, 26/05/89).

Of special interest to Chelsea Ltd are frauds based on the CHAPS system. Large scale frauds have been committed over such systems in the past. It is alleged that in 1988 there was an attempt to transfer £32m from the London branch of the Union Bank of Switzerland via the SWIFT[6] Electronic Fund Transfer system (Investors Chronicle, 26/05/89). Such a fraud would have potentially disastrous consequences for Chelsea. Unlike paper-based frauds, the difficulty of EFT-based frauds is not affected by the sum involved: it is no more difficult to embezzle £100m than it is to embezzle £1 by direct transfer. The only limit on the amount a successful fraudster could potentially remove by EFT is the credit limit in the company's account.

Hacking

Hacking can be defined simply as unauthorised access to a computer system. It is sometimes split into two categories, the names of which are subject to long-winded semantic debate among the hacking community. Briefly, 'Tappers', such as those involved in the Virgin/BA case (Computing, 14/01/93), are unauthorised users who target a specific system in order to unlawfully gain information of value, while 'Crackers' such as Paul Bedford ('Independent', 26/02/93, p.3) are unauthorised users who, although uninterested in the content of a system, attempt to hack into it for the challenge.

Both types of hackers are a problem for the security of a system. Because hackers usually gain a high level of system privilege, it is very difficult to gauge exactly what data or applications may or may not have been altered. An investigation is very time-consuming and costly, and usually forms the main cost of any hacking attack. The NCC survey identified hacking as (on average) the most expensive form of attack to detect and recover from.

The extent of the hacking problem is very difficult to gauge. Estimate of the numbers of hackers in the UK range from 8-10 serious hackers (Hugo Cornwall) to 50 serious hackers and 10,000 enthusiastic 'amateurs' (Corrupt Computing Bulletin Board, 1990). The knowledge required to become an enthusiastic amateur is simple to obtain. Details of loopholes and exploitable vulnerabilities are freely available on many Internet sites.

The Chelsea Security Manager's attitude[7] that hackers can break into NASA computers, so there is no point in trying to keep them out of commercial systems, is dangerous. It is true that many crackers are dedicated and resourceful people, and given enough time could break into most systems. However, unless they have a special interest in a particular system, when faced with efficient security, they will usually turn their attentions elsewhere. Combating hacking is not a case of making a system 100% secure, but of making a system secure enough that the time and resources needed to break in are more expensive than the value of the information gained.

For an in-depth study of hackers and hacking, refer to the 'Hackers Handbook' (Cornwall, 1985), or 'The Hacker Crackdown' (Sterling, 1992).

Rogue Programs

Rogue Programs, usually generically referred to as viruses, are unauthorised programs that usually act to the detriment of their host system. Viruses are the most common form of rogue program and have received the most publicity. A virus is a piece of code that attaches itself to other pieces of code, such as applications software, and that can replicate itself. Other forms of rogue program worth noting are: Trojan Horses, which masquerade as authorised programs; logic bombs and time bombs, destructive routines set off when particular logical criteria are met; and Worms, which are similar to viruses, but are 'free-standing' pieces of code that do not need to attach themselves to other code. Although useful viruses and worms do exist (Hafner and Markoff, 1991), these have never been given the same media exposure as their malignant siblings. The majority of viruses discovered to date have either deleted or modified data held in the system, or caused denial of service.

Viruses have undoubtedly the highest public profile of any security threat. The publicity given to the Michaelangelo virus, the Friday the 13th virus and others has raised public awareness of the problem. Of particular note are the increasing number of viruses coming out of Bulgaria following its recent IT boom (alt.security,1994), and the freely distributed virus software engineering tools available from bulletin boards, which allow novice programmers to write effective viruses.

Hoffman (1990) provides a complete description of the capabilities, underlying theory and means of prevention.

[6] Society for World-wide Interbank Telecommunications.

[7] see Appendix A

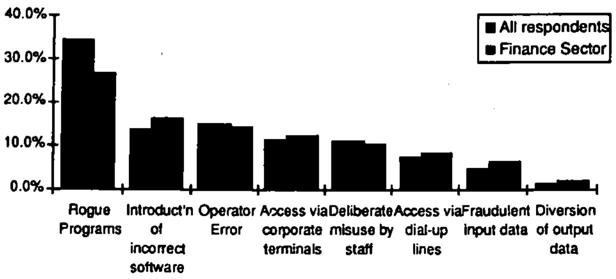
The Motivation behind Crime

If the motivation behind crime can be understood, then security procedures can be aimed specifically at preventing this motivation from producing fraud.

Jack Bologna, president of George Odiorne Associates, Michigan, has researched motivations behind white collar crime, with particular reference to computer crime. He listed 25 reasons for theft and asked corporate victims of theft which reasons they believed to be valid. The two most common statements were:

- They feel that they can get away with it and not be caught.
- They think that stealing a little from a big company won't hurt.

Figure 2.3 Logical Breaches by Type



Source: NCC Survey 1991

One widespread reason for the first statement was the belief that most breaches are discovered by accident rather than audit or design.

Bologna has constructed eight basic personality types which he claims cover all eventualities. He says that only people from four of these eight categories might be tempted to steal under the right circumstances. Furthermore, these four categories represent at most 20% of the population.

Both of these statements apply to Chelsea Ltd. With the minimal amount of security present, fear of getting caught is unlikely to deter any potential fraudster. Such is the nature of Chelsea's business that large sums of money are being traded regularly. When faced with million-pound deals, employees are likely to believe that the company will 'not even notice' the loss of a few thousands. Unfortunately, this is not the case. The money being traded generally belongs to investors, not the company, and a 'few thousands' here and there would eat heavily into their profit margin.

To be continued in the next issue of CASG Journal

STOP PRESS . . . STOP PRESS . . .

BCS ANNOUNCE BCS NET

With this edition of the Journal you will find a brochure giving details of the Society's new electronic mail and Internet connection services. This is only available to BCS members, but you will also find an application form for Affiliate member status. If you want a few extra letters after your name, why not become an AMBCS and get wired at the same time?

We have arranged for the BCS people responsible for membership and the new BCS Net to provide us with more details in our Summer edition.

Letters to the Editor

Sir,

"The Independent" seems to have been a touch gullible when Steve Fleming came up with his "BT secrets" story, and you are right to treat it to some editorial wrath in the Winter edition of the Journal. On the other hand, there seems to be a danger of over-reacting. Isn't it quite useful for newspapers to run stories which at least make people stop and think about their computer security?

I would also take issue with the conclusion you draw from this particular case. To claim that "the small minority of information thieves and abusers must be balanced against business efficiency" seems very dubious. What this incident demonstrated was how quickly a simple opportunity offered to just one of this "small minority" can lead to mayhem. I wouldn't wish to develop the kind of paranoia shown by some journalists, but surely we all need to mull over a few things which are likely to keep us awake at nights. Among these I would definitely include the risk of giving temporary work, with inappropriate systems access, to an aspiring hacker.

Yours sincerely

Andrew Hawker
Department of Accounting & Finance
University of Birmingham

PROVISIONAL MEETING SCHEDULE FOR 1995/96 SEASON

12th September 1995 (16.00 for 16.30)	**Control of Contract Staff**	Mike Cullen Chairman BCS Independent Computer Contractors Specialist Group
10th October 1995 (16.00 for 16.30)	**Controls in a Futures and Derivatives Trading Environment** (Joint meeting with ICAEW IT Faculty)	Steve Bullen RABO Bank of The Netherlands
7th November 1995 (full day)	**Contract Management, Negotiation and Control** (Joint Meeting with BCS Legal Specialist Group)	Jeremy Holt Charles Russel Solicitors
12th December 1995 (16.00 for 16.30)	**Use of Human Resource Systems to Manage Access in a Heterogenous Environment** Joint Meeting with BCS Security Specialist Group)	John Ford/Paul Munford Safeway Plc
16th January 1996 (16.00 for 16.30)	**Audit Implications of Client Server**	Price Waterhouse
13th February 1996 (full day)	**Third Party Project Development and Support - Control & Audit Issues**	FI/Logica/ITNet
12th March 1996 (16.00 for 16.30)	**Audit & Control in a Windows Environment**	Stan Dormer System Security Ltd
8th April 1996 (16.00 for 16.30)	**Annual Debate with ISACA Topical Motion**	TBA
14th May 1996 (full day)	**Discussion Group** Topic to be announced	TBA
14th May 1996 (17.00)	**Annual General Meeting**	

casg
Computer Audit
Specialist Group

THE

ANNUAL GENERAL MEETING

OF THE

COMPUTER AUDIT SPECIALIST GROUP

OF

THE BRITISH COMPUTER SOCIETY

WILL BE HELD AT

5.00 PM, WEDNESDAY 10th MAY 1995

AT

BCS, 7 MANSFIELD MEWS, LONDON W1

(Nearest tube stations are Oxford Circus & Regents Park)

AGENDA

1. Approval of the minutes of the AGM held on 11th May 1994
2. Chairman's Report
3. Treasurer's Report
4. Election of Officers
5. Election of Auditor
6. Appointment of Committee
7. Plans for 1995/1996
8. Any Other Business

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

NOMINATIONS FOR THE MANAGEMENT COMMITTEE

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

We hold about six committee meetings a year at a London location. The meetings start at 5.00 pm and we try to finish them by 7.00 pm. 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 John Mitchell (01707 654040), Raghu Iyer (0171 236 8000) or any other committee member (their telephone numbers are given elsewhere 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.

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

John Mitchell

THE BRITISH COMPUTER SOCIETY COMPUTER AUDIT SPECIALIST GROUP NOMINATIONS FOR THE 1995/96 COMMITTEE

Position: . . . .

Nominee: . . . .

Proposer: . . . .

Seconder: . . . .

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

casg
Computer Audit Specialist Group

Management Committee

CHAIRMAN	John Mitchell	LHS - The Audit & Control Consultancy Email: jmitchell@lhs.win-uk.net	01707 654040
SECRETARY	Raghu Iyer	KPMG Peat Marwick McLintock Email: raghu.iyer@kpmgmark400.gb	0171 236 8000
TREASURER	Nigel Smith	NJ Associates	01707 334421
MEMBERSHIP SECRETARY	John Bevan	Audit and Computer Security Services	01992 582439
JOURNAL EDITOR	Rob Melville	City University Business School Email: SC355@CITY.AC.UK	0171 477 8646
MEMBERS MEETING	Paul Howitt	Tesco Stores Limited	01992 644250
	Jenny Broadbent	Cambridgeshire County Council	01223 317256
DISCUSSION GROUPS	Bill Barton	The Rank Organisation PLC	01883 623355
	Steve Pooley	Independent Consultant	01580 891036
	Alison Webb	Independent Consultant	01223 461316
	Jim Ewers	Hertfordshire County Council	01992 555328

Membership Enquiries to:
John Bevan
46 Queens Road, Hertford,
Herts SG13 8AZ

01992 582439

COMPUTER APPLICATIONS SYSTEMS AUDIT WORKSHOP

Objectives

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

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

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

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

Who Should Attend

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

Course Programme

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

Topics covered will be:

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

Date : **13 – 14 June 1995**

Venue: **Swallow Royal Hotel, Bristol**

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

Non-members: **£630 + VAT**

Note: This workshop is fully residential

Contact:

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

Tel: 0171 498 0101
Fax: 0171 978 2492

casg
Computer Audit Specialist Group

The British Computer Society

PLEASE RETURN TO
John Bevan
Membership Secretary

46 Queens Road
Hertford
Herts SG13 8AZ

Membership Application/Renewal

(Renewals are due in August of each year)

I wish to APPLY FOR / RENEW (delete as appropriate) my membership of the Group in the following category and enclose the appropriate subscription.

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

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

INDIVIDUAL MEMBERSHIP (A member 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 Proccssor
4 = Academic
5 = Full-Time Student
6 = Othcr (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:

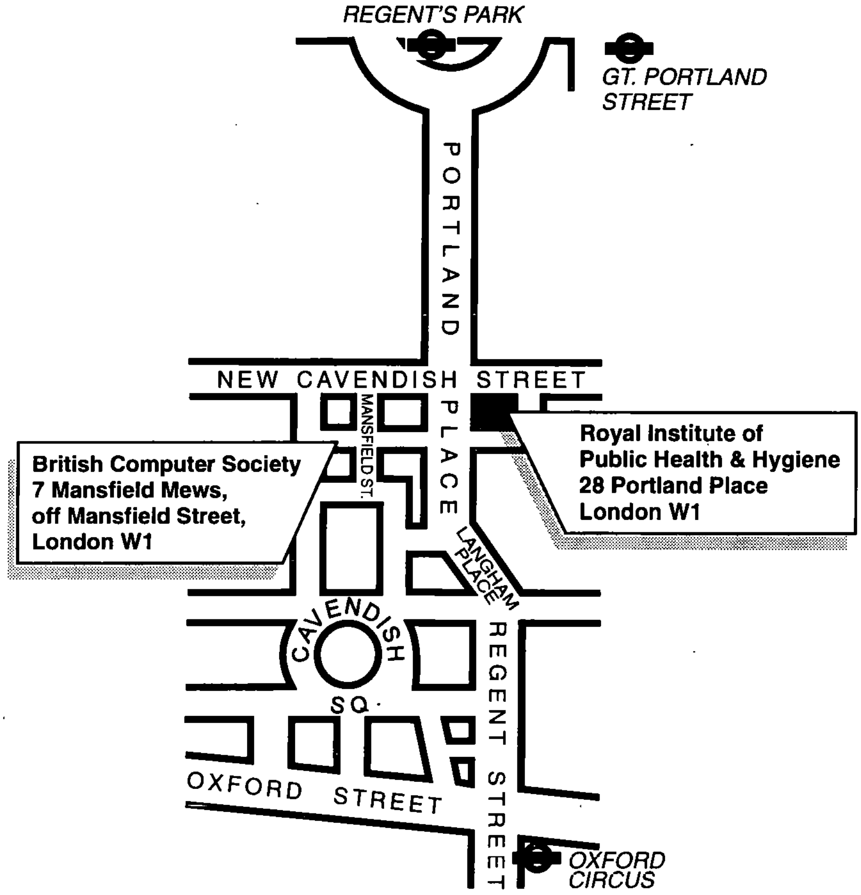
ADDRESS:

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

Venues for Members' Meetings



British Computer Society
7 Mansfield Mews,
off Mansfield Street,
London W1

Royal Institute of
Public Health & Hygiene
28 Portland Place
London W1

SUBMISSION DEADLINES

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