ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 7 NUMBER 1 AUTUMN 96

The British Computer Society

Technical Briefings 1996/97

8 October 1996
Auditing and automation

To be held jointly with the IT faculty of the ICAEW at their premises in Moorgate Place

Chairman	Paul Williams: Partner, Binder Hamlyn
Automating UNIX Audits	Mike Chorley, Trillion Software
Viruses from the Internet	Joseph Richardson, Dr Solomons
Data Matching	Simon Keane, London Team Against Fraud
Implementing automated working papers	Ken Ebbage, Pentana
Evaluating against BS7799 using COPIT	Andrew Birkbeck, Glynwedd Steel Ltd

---

Tuesday 14 January 1997
Networks: moving ahead securely

Royal Aeronautical Society

ATM and security	Leslie Hanson, Cabletron Systems Ltd
Open doors into networks	Rose Hines, IT Vulnerabilities
Moving to Novell 4: Security Implications	Peter Wood, First Base
Secure Gateway implementation	Yag Kanani. KPMG

Tuesday 15 April 1997
Systems development audit: Adding value

Royal Aeronautical Society

Diagnosing project problems, Signs and Symptoms	Ruth Woodhead, Admiral Management Services
Systems Development audit: The IS manager's view	Graham Folmer, Addenbrookes Hospital
Testing the Testers	Dorothy Graham, Grove Consultants
Preventing problem projects: the auditor's role at the outset	Geoffrey Smart, Coopers and Lybrand
Auditing RAD	Stan Dormer, Stan Dormer Associates

Contents of the Journal

ADVERTISING IN THE JOURNAL

Reach the top professionals in the field of EDP Audit, Control and Security by advertising in the CASG Journal.
Our advertising policy allows advertising for any security and control related products, service or jobs.
For more information, phone John Mitchell on 01707 851454.

Editorial Panel

Executive Editor
John Mitchell
LHS – The Business Control Consultancy
Tel: 01707 851454
Fax: 01707 851455
Email: jmitchell@lhs.win-uk.net

Academic Editor
George Allan
Portsmouth University
Tel: 01705 876543
Fax: 01705 844006
Email: allangw@cv.port.ac.uk

Book Reviews Editor
Iltaph Khaliq
Royal Bank of Scotland
Tel: 0171 427 8751
Fax: 0171 427 9953

Product Reviews Editor
John Silltow
Security Control and Audit Ltd
Tel: 0181 300 4458
Fax: 0181 300 4458
Email: john@scaltd.demon.co.uk

BCS Editor
Colin Thompson
British Computer Society
Tel: 01793 417417
Fax: 01793 480270
Email: cthompson@bcs.org.uk

The ***Journal*** is the official publication of the Computer Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

Letters to the editor are welcome as are any other contributions. Please contact the appropriate person on the editorial panel.

Editorial address:
47 Grangewood,
Potters Bar
Herts, EN6 1SL

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

EDITORIAL

Having survived my first year as editor without so much as receiving a single letter, congratulatory or otherwise, I enter my second year with a touch of trepidation. Is all my bullying of my sub-editors really a waste of time? Would anyone miss the *Journal* if it did not come out on time? Does it add any value to the common body of knowledge? I found that I could answer all of these questions in the affirmative (yes, to our American cousins), simply by the publication of the article on CICS Table Auditing which you will find inside this edition. It is certainly not an area that I have ever tackled and yet its control implications for most installations is probably greater than the concern we have with many other areas. Likewise, the refereed item dealing with Computer Use and Misuse provides a useful starting point for those in the readership who would like to separate the myth from the reality. It is likely that neither of these articles would have seen the light of day without the existence of this *Journal*. So I now feel justified in bullying all those people who make this *Journal* possible.

The Java programming language has come from nowhere to being one of the most widely used languages for the Internet. In this edition, John Silltow reviews one of the latest books describing this new language.

During the last fifteen years I have been privileged to witness the introduction of desk-top computing, the explosion in the communications arena, the growth of multi-media and now the explosion of the Internet. Four major advances in less than a human generation and the newest one seems to have become established far quicker than the previous three. Indeed, it really needed the previous advances to take off.

This rapid change makes it even more important for us computer auditors to keep up to date. Alison Webb raises this issue in the Chairman's column, where she explores the problems of control in a client/server environment, but the wider problem needs to be tackled by everyone who sees computer audit as a profession.

The BCS is pushing continuous professional development and although I support the concept, I consider that the way they are approaching it will be too bureaucratic and restrictive in this fast moving world. I much prefer the approach taken by many other professional bodies, including both the ICAEW and the Information Systems Audit and Control Association, where knowledge acquisition does not need to be approved of in advance, but is ratified in arrears, with the onus on the individual to keep the necessary records. Rather like self assessment for income tax. Now if that is good enough for the government, then it should be good enough for the BCS!

By the way, did you notice in the movie *Independence Day*, that the reason the aliens lost the war was simply because they did not have virus protection implemented on their enterprise server? Silly creatures. Obviously no computer auditors amongst them!

John Mitchell

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

Chairman's Corner

Alison Webb

Complex technologies like client/server can be the most interesting computer audit work there is: but like anything complicated, actually defining what they are can be difficult. I was talking to someone the other day who felt that client/server was really hardly more than a new name for existing services, and that its impact on users was largely confined to using a PC instead of a dumb terminal to access corporate applications, and remembering to call the mainframe the corporate server. It's easy to understand why the emphasis has been on PCs: their processing power and affordability means they are now ubiquitous. It's worth noting, though, that the core applications on standalone PCs haven't really changed much in the last ten or fifteen years: word-processing, spreadsheets and small databases. What has changed, of course, is the processing power.

Comparisons between today's PC and yesterday's mini or even mainframe are often to the PC's advantage, and we're using this extra power to make the tasks we've always done easier. Word-processors, for instance, are a world away from what they were ten years ago. PCs have developed skills at interacting with users that mainframes have never had: which is why we are front-ending our existing core mainframe applications with smart new GUIs. It's perhaps the cheapest and most effective way to improve productivity and cut down on user errors without entirely re-designing our systems. But underlying what we see and experience as the features of client/server systems are the programs and processes we use to relay our data from one machine to another. One thing about client/server computing that as auditors we mustn't forget is that it involves the exchange of information between two processes on different computers. If we substitute "two people exchanging information" or "a process and a user exchanging information" which are the same thing in principle: then we're on to familiar audit territory: we have concerns about authentication and authorisation. A major, but largely undiscussed, audit concern when dealing with client/server architectures is the authentication of remote processes. How do we know that the client process, which may be installed on a PC on the other side of the country, or the world, is really allowed to get data from our corporate database,

perhaps to change it? We don't know who is running the program on the PC: we can't see who is sitting there and so check they're on our list of authorised users. Can we be sure that the software on the PC has remained unchanged? It may have been replaced by a rogue program, if access to the PC itself is poorly controlled.

There are solutions to our problems like Secure RPC, which uses a mixture of encryption techniques and the familiar password check to help the server validate the messages that come from the client process. However, at least in my experience, not a few communication methods don't stick to secure and well-tested session protocols, but use their own home made variations. These usually pay lip-service to security, but often miss the point, typically by holding passwords (encrypted if you're lucky) on user PCs; or by implementing password checks in such a way that regular password changes become administratively virtually impossible. We need to think through these issues, because it's our job to advise on just how secure systems need to be: and decisions will be difficult here, because there aren't just set-up costs to be considered. Using encryption and secure authentication will be a permanent system overhead. CASG are including a Client/Server session in the Technical Briefing on 14 January 1997. We can start to think through the issues then, but we also need your views on how else we can help our members get the information they need, and the right forums to discuss key issues.

Please let us know!

CICS Table Auditing

David M Judge

The most important on-line systems running in large businesses today are written around a teleprocessing monitor like IBM's CICS. These are the applications that are the lifeblood of any corporation and often run 24 hours a day. Indeed any problem with these applications or the software that controls them will cause major disruption to the business operation or, in extreme cases, its complete breakdown with severe consequences.

Therefore a major concern for a computer auditor is how do you track and control changes to your CICS Systems so that you can assure management that only authorised changes are being implemented? Maybe you don't - or maybe you just track the changes to the source programs and the implementation of load modules into production. But CICS is managed and controlled by a number of tables without which no application can be run. In many installations hundreds of table changes are executed every week and the management and control of these CICS table changes is non-existent in most organisations.

Why should this be? After all a great deal of effort is put into planning for recovery from major physical disasters like fire or machine breakdowns. A software problem is clearly not so visible to senior management but it can be no less disastrous to the business and if the right information is not available it can be even harder to resolve. Many of these so-called legacy systems are highly complex, having been developed and modified over several years, so that it may be necessary to call on many areas of expertise before a satisfactory solution is found.

The main reason why no sensible approach is taken to track and audit these critical applications is that there is a total lack of easy to use facilities for obtaining information and providing reports in a timely manner, or enabling the right questions to be asked. Indeed too many products leave the user to develop and maintain records by utilising lengthy and highly technical procedures. It is therefore not surprising that most users see this area of maintenance as difficult and time consuming. They will go to great lengths to avoid it in the hope that serious problems only happen to other people and never in a well-ordered shop like theirs.

So what are the real issues and how can we take the pain out of securing, controlling and tracking these complex but vital applications?

The crux of the problem is that the CICS table change process, the routine needed to create and maintain CICS resource definitions, is often slow, labour intensive, dominated by paper and prone to mistakes.

There is a lot of looping activity between the application and CICS system programming groups due to assembly errors, improper or incomplete table definitions and the use of duplicate program, transaction and group names. Sometimes errors are not detected until the updates are applied to the CSD or the RPL, causing the request to be returned to the requesting programmer to repeat the update processing.

Clearly in such a manual process it is difficult and laborious to create paper audit trails, contact lists, backout procedures and operational notification, the very information that is required by auditors. The result is that the data maintained is usually inadequate, inaccurate and out of date.

One way to address these issues is to apply some degree of automation to the CICS table change process. By eliminating the paper flow and personnel in the middle, an automated on-line CICS resource management system could move changes from the application programmer through approval and into production in minutes. CICS System programmers would thus be relieved from having to code, test and implement table changes and could concentrate on more important development work. Productivity would be improved thus relieving pressure on an ever diminishing specialist resource. Furthermore, as a by-product of the change process it would not be difficult to deliver a solution to the audit issues mentioned above and to collect, in a single database, all the necessary change information which could then be queried to supply additional information required by the auditor.

Automation alone is not enough. It is necessary to lay a change control process over the many CICS table updates that get generated for test and production regions. Such a CICS change management system needs to address the key issues that concern Auditors of CICS applications. These issues fall under three main headings - security, control, and tracking & reporting.

Security - All MVS computer installations use one of the popular security products like RACF, ACF2 or Top-Secret thus any automated change management system needs to work with the existing security environment .

Multiple levels of security are needed to provide maximum flexibility in controlling each user's access at table, function and attribute level. Indeed it is desirable that access be granted at the site, region, support level (test/production), application, group and table level.

If Application Programmers are to be given the ability to input directly their change requests it is important to be able to tailor dynamic views on the access panels. Dynamic views permit you to show the right table attribute information to the right audience. Thus an Application Programmer may be able to see several attributes but only update those for which he is authorised while a CICS Systems Programmer is permitted to update all of the attributes. These profiles need to be tailored at the individual level.

An example of this would be to imagine that a change to an HR application has taken place under unusual circumstances resulting in some data associated with personal information being tampered with.

Under normal circumstances it would be difficult to track and isolate the specific person responsible for the change. An automated system could very easily allow the user to trace the authority levels of all those able to alter a particular table and then identify the person responsible for the action.

The authority of each user must be controlled from a central point, and once given, the activity of each user can be recorded and easily tracked on a regular basis via reports. It must also be possible to do this in an emergency or unusual situation.

Control - Any new change control system must provide the same functions and facilities for controlling CICS table changes that are most likely already in place to manage source program changes. Indeed interfaces to other change management products such as Endevor and Change Man are desirable so that only a single change action is required to complete a change process.

Automation usually supplies a new discipline but it is also necessary to maintain maximum flexibility. Changes can be treated in a variety of different ways depending on policy or circumstances. They must be able to be post- dated, approved, held, rejected, cross-checked and activated. In addition it is necessary to provide automated back out by change control number, preferably with regression testing. All these movements need to be logged, date-stamped and marked with the USERID of the person doing the maintenance.

No packaged system can be just dropped into a complex environment. Every installation has its own standards, for example naming or transaction. Thus we must be able to include routines that will adapt the package to the particular situation. Data entry exit points are a must, permitting the rigorous enforcement of installation transaction or naming standards. They can be used when adding or changing definitions, creating a change control number or returning from a security call. Installation defaults for table attributes can thus be established for creating new entries and each application or work group can have different defaults.

Finally it is clearly desirable to provide a single centralised point of control for all CICS table maintenance. From a single database it should be possible to manage table entries for both local and remote sites. Thus all table maintenance can be done from the host site, eliminating the need for CICS staff at remote sites, reducing costs and increasing control.

Tracking & Reporting - The key to providing an audit trail is to allow the tracking of all changes, status, contacts, and counts at region, application, group, type and entry name level. All maintenance activities need to be date stamped in the yyy-mmm-dd-hh-mm-ssssss format with the USERID of the person doing the maintenance. It must be easy to obtain such information as who last changed a table entry, when the CSD was last updated or when the region was last cold-started. When problems arise help desk personnel must be able to query a database to determine who has responsibility for the transaction, application, region or table entry.

An automated system allows the maintaining of a wealth of information on its database enabling queries to be made using either the standard set supplied or those defined by the installation. Frequently used reports would become a part of the standard process, preferably with wildcarding, so that control information on changes or contents of regions are always available.

In addition it is also important to allow ad hoc requests to be made using a simple query language like SQL to address the emergency or one-off requirement. This is easily achieved if the system is built around a recognised database product like DB2.

Thus a system designed to help the CICS Systems Programming staff to automate the table maintenance process can be extended to lay a change control process over the many CICS table updates that get generated for your test and production regions. In so doing it can produce a wealth of information vital to the audit process.

In the USA efforts have been made to address these requirements with a product called CATS (CICS Automated Table System) from Emprise Technologies of Pittsburgh. CATS is already in its ninth release and is widely used in both large and small businesses. Now available in Europe it is already installed in accounts in Scandanavia, France and the UK.

David Judge is a consultant with Emprise Technologies Europe. He is profiled in this edition. For further information on CATS see the enclosed mailer or contact EMPRISE TECHNOLOGIES EUROPE - 01278-795404.

Worth Interviewing?

One of my clients received the following unsolicited job application - Ed.

Dear Personnel Officer,

I am writing in the hope that you will consider me for a job as a computer auditor to utilise my experience in IT.

I own a Tandy Laptop PC with DOS 3.3 and Deskmate Windows which I find very useful for word processing, keeping tabs on my finances and teaching my nephew and niece. A number of batch programs have been written for the purpose of backing up the data and tailoring the system functionality. I'm reading books on apprehending (sic) how the Stock Market operates, perceiving MS DOS 3.3 and what the Internet is all about. After I was persuaded to visit a gathering to listen to a 'Master' from India, I've become intrigued - hence I purchased a book entitled: The Path of the Master. Listening to talk show radio is an excellent means of keeping abreast of current affairs.

A total of five years has been spent in the IT sector using ITL Stratus minicomputers and TML/COBOL computer languages, primarily as a maintenance programmer.

I will be going to college for a one day session on Novell Netware introduction.

I would be very pleased to attend an interview to discuss a position and can be contacted by letter at the above address.

Well, anyone who can 'apprehend' those stock market guys from a lotus position must have a role in computer audit, but I'm not sure what it is - Ed.

Computer Use and Misuse

by

George Allan & Suzanne Salter

Abstract

This paper outlines the main areas of computer abuse and misuse. It addresses intentional unauthorised access and covers sabotage and theft. The software attacks discussed include viruses, Trojan horse and worm. The paper also categorises types of criminal including the fraudster and hacker, and progresses to discuss the Compute Misuse Act (1990) and definitions of offences. Finally, some of the main authorities against computer crime are profiled and include FAST, BSA, DPA, Computer Crime Unit and ELSPA.

Keywords: *Computer Misuse, Hacking, Fraud, Virus, Unauthorised Access, Computer Misuse Act, Computer Security, Threats, Vulnerabilities, Risk Analysis, FAST, DPA, ELSPA.*

George Allan holds the post of Senior Lecturer in the Department of Information Science at the University of Portsmouth, Hants, England and is well known for his views and expertise in computer systems development project management.

Suzanne Salter is a graduate of Portsmouth University and is currently with Ericsson Business Networks. She is working on international contracts one of which is the great man made river project in Libya.

1.0 Introduction

During the last decade there has been a marked increase in opportunities and expertise for computer misuse in nearly all facets of computer technology. In the wrong hands a computer can provide a very easy way to commit crime. Society has gained as computers have become faster and easier to operate. Information can be retrieved in seconds and moved around continents at the click of a button thus facilitating communication in a way never possible before. The rapid growth of computers has raised many questions regarding computer misuse. Not only are computers targeted for misuse but are also instruments in the committal of crimes.

2.0 Background

Forms of computer misuse include software piracy, data manipulation, planting of viruses, unauthorised access, hacking, theft (of data and hardware), sabotage, deliberate aggression against the computer and even terrorism (whether or not the computer is used as an unwitting accomplice or is the target of the crime). These are a few of the serious threats to every organisation which uses automated systems and are threats that will continue to grow. Computer misuse also includes such acts as harassing, transmitting offensive material, obscene jokes/ethnic slurs and developing chain letters.

Current Costings

The cost of computer crime is not easy to assess but breaches in computer systems security are estimated to cost UK companies over £1.2bn each year according to a 1991 Department of Trade and Industry survey. The cost of software piracy is difficult to calculate as no-one really knows how many copies of games/WP packages etc. have been illegally made. Losses relating to fraud are perhaps easier to quantify than illegal software copies.

The DTI survey shows that since 1990 crime against computers has trebled. Eight times more illicit software is now in use than in 1990. Fraud increased 38% on 1990's figures and reported incidents soared by 183%, costing firms £28,170 per incident compared to £17,080 three years ago (R. SIZER 1994) - almost a 65% rise.

The survey also shows that 80% of the 950 companies responding had suffered a breach in the past 2 years. The average cost per incident of a computer security breach is estimated at £9,000.

3.0 Types of Computer Misuse

The basic characteristics of computer crime are intent, disguise of purpose and concealment. Common computer abuses are listed below in categories. This covers most of the past and present issues relevant in the Industry, and is far from being exhaustive.

3.1 Computer Fraud

Fraud is defined as any act(s) intended to deceive or mislead others and resulting in loss / gain for the victim / perpetrator, respectively.

Fraud committed with the use of a computer is on the increase faster than all other categories (BENBOW 1992). This can be attributed to increased levels of computer literacy and is mostly committed by employees inside a company.

The potential to commit fraud is based on opportunity and motive; the use of the computer as a tool may be incidental or core to the entire fraud. The computer is never deceived itself, it merely carries out the instructions given.

Computer fraud falls into three categories:

- Input fraud
- Program alteration/manipulation
- Output fraud

3.1.1 Input Fraud

Falsification of data during input is cited as the simplest and most common computer fraud (HOAD 1992). The fundamental

principal behind input fraud is that records are deliberately added or deleted or otherwise altered at input stage. It should be pointed out that genuine mistakes can and do occur.

3.1.2 Program Alteration/Manipulation

Manipulation of a computer program is not as common since a higher level of technical expertise is generally required. Systems programmers can be highlighted for their intimate knowledge of operating systems and programs. A common form of fraud during processing is the deliberate manipulation of master files. False entries can be added resulting in false credits being created. "Housekeeping" activities - often carried out by one person - can be an ideal opportunity to defraud. "Salami" fraud is another method whereby small amounts from large volumes of accounts are "sliced" off, typically by rounding fractions.

3.1.3 Output Fraud

HOAD (1992) cites that because computer output is normally accepted as being accurate and genuine, its authenticity is taken for granted. Output can be stolen or falsified to cover thefts which may have taken place back down the line or to postpone detection. One case in the USA involved an operator who pushed the "print" key 39 times when his own pay cheque was being processed and then presented them for encashment.

As many companies every year are being attacked from within, the Metropolitan Police teamed up with IBM to produce a computer crime leaflet titled "Don't let them get away with I.T." to make staff realise that tampering with company information *is a criminal offence*. (The Computer Misuse Act, 1990 is discussed later in this report). Output fraud is the least common type in this category.

3.2 Intentional Unauthorised Access

Gaining access to another's computer without consent comes under this heading and constitutes an offence criminalised under the Computer Misuse Act (CMA) as Unauthorised Access. Causing a computer to perform any function with intent to secure access to data in that computer when the access is unauthorised is common.

3.2.1 Hacking

Hacking is described as deliberately setting out to explore a system without entitlement to access. The earliest hackers were students at the Massachusetts Institute of Technology (MIT) in the late '60s who specialised in tracing the wiring of the MIT network using pieces of telephone circuitry. Hacking has resulted from world-wide use of standard communications equipment which allows systems to be interconnected and thus began to emerge with the development of time-shared systems. Hacking has received considerable media attention in recent years and more recently has acquired the term "cracking" - those who use computers for illegal, unauthorised or disruptive behaviour (JOHNSON 1994).

FORESTER & MORRISON (1990) suggest hacking is about intellectual challenge, not malicious damage - hackers seldom *steal* from their victims. They term it as "any computer-related activity which is not sanctioned or approved by an employer or owner of a system or network".

Techniques used to hack into computer systems include:

- piggybacking
- scavenging
- browsing

Piggybacking involves tapping into communications lines and riding the system behind a legitimate user. Scavenging involves looking for stray data for clues that might unlock secrets of the system. Unauthorised browsing also constitutes an offence.

3.2.2 Eavesdropping on a Computer

This is distinct from hacking as it does not entail obtaining *access*. Complex techniques of eavesdropping include bugging telephone wires carrying data; eavesdropping on electromagnetic fields generated by a screen (which can then be recreated under the right conditions); or more expensive forms of microwave communications capture.

3.2.3 Misuse for Personal Gain

The activity of obtaining information for personal gain is clearly for cases of industrial espionage. This would highlight the row between Virgin Atlantic and British Airways (BA) where the latter poached customers from Virgin by accessing (Virgin's) computers. It was also found that using similar techniques, BA may have been instrumental in Air Europe's collapse in March 1991. It is suspected that even some of the Police Forces in the UK abused the Police National Computer System by accessing it to pursue domestic disputes and check up on daughters' boyfriends (Computing 1994).

3.2.4 Masquerading as a legitimate user

When a password is stolen the unauthorised user will be in a position to secure access to a specific computer/network and masquerade as the legitimate user.

3.3 Sabotage and Blackmail

Acts of computer sabotage usually happen when the empowered become the embittered - when workers, out of sheer boredom or inadequate training, "turn their computers into tools of mischief and mayhem" (SPROUSE 1993).

Sabotage can be subtle or downright obvious. Examples include a programmer at the Bank of America who, blamed for sloppy and slow work, proceeded to rewrite the payroll system so it would delete itself during run-time. The 600 computer personnel in Denmark who went on strike for four months in 1986 paralysed the government and caused the ruling party to table a general election. This was regarded by some as an act of sabotage; such actions turn the possibility of blackmail into a real threat.

3.4 Denying Access to Authorised User

Denying access to an authorised user may involve alteration or deletion of legitimate passwords or physical prevention - for example a locked door. Similarly software may be written to handle only a certain number of users; even occupying a computer port can obstruct legitimate users.

3.5 Unauthorised Destruction/Alteration

Destruction of programs can be achieved by physical removal of devices (disks/tapes) or electronically by degaussing whereby the media are demagnetised. Other more elaborate forms of deletion include overwriting with zeroes or other characters on entire disks/tapes to render them useless. Alteration can also include changing assessment grades at Universities/colleges.

3.6 Software Theft

Software theft manifests itself in many ways including mail order rackets, corporate overuse, counterfeiting of popular packages and copying for home use. Distribution of illegal software is facilitated using technologies like bulletin boards, CD ROM's and the Internet. "Software piracy" is fast becoming a booming business in its own right due to considerable amounts of money which can be made by individuals. Last year over $40m worth of illegal software was seized in the UK alone (FAST May 1994). Figures from 1993 show the software industry lost £3.3bn in Europe from illegal software use. The Independent reported on 27th May 1994 a rise to £8.5bn in 54 countries. Industry bodies have been set up to fight this increasing threat. The Business Software Alliance (BSA) enforces anti-piracy action internationally and the Federation Against Software Theft (FAST) controls software theft.

In 1991, a European directive was introduced which brought software copyright into force and, as a result, saw the use of pirated software in Europe drop from 77% in 1991 to 61% by 1993. In 1992, 86% of Italy's software market was illegal; Mirror Group Newspapers and Trent Regional Health Authority (in 1993) admitted to illegally copying software. In Indonesia, Pakistan, Thailand and the United Arab Emirates, 99% of software in use is reported to be illegal (The Independent, 23rd May 1994).

Piracy of games software is also a growing problem. The Sunday Times on 26th June 1994 reported a man found to be illegally copying computer CDs - allegedly containing £10m of pirated software.

3.7 Software Attacks

Most (if not all) computer systems are susceptible to attacks on their software because of the volumes of software exchanged between users. Recently there has been increasing attention given to the software designed to threaten the security of computers:

3.7.1 Viruses

The term "virus" was first used to refer to any unwanted computer code but now typically refers to "rogue code" - a segment of machine code that will replicate itself wherever and whenever possible throughout a system or network. Virus Bulletin is a publication which lists pages of current and new viruses. The DTI estimates an annual cost of £128 million to UK companies for virus infections.

3.7.1.1 Key Characteristics of a Virus

Computer viruses share many characteristics of biological viruses and can be viewed, given the reproductive life cycle, as a computerised life-form. A virus can mutate or copy itself. Commonly viruses are introduced by free disks given away with magazines. If an "infected" disk is inserted into a PC the virus may copy itself onto the hard disk and subsequently any floppy disk used thereafter. Many viruses incorporate a latency period where an event or date will trigger their harmful actions. Viruses are *permanent* - residing on a hard disk until eradicated (by use of a software "vaccination"). Viruses can cause many effects from writing trivial slogans on the screen to horrifying system crashes.

3.7.1.2 Specific Viruses

There is some dispute concerning the first viruses created. Fred Cohen claims the first virus was "born" on November 3, 1983 written by himself for a Security Seminar. Subsequently he published his results at the 1984 National Computer Security Conference stating he had established a virus which could infect systems in only a few minutes. Susan Headley, a Las Vegas hacker, claims to have helped create the world's first virus in 1980. Subsequently, many viruses have been designed and detected and are variously named or numbered. Some viruses are intended to do nothing more than amuse: like the cookie monster program that forced users to spell the work "cookie" before access to files was granted. The Pathogen virus was more dangerous. No doubt to the delight of Red Dwarf fans, it displayed the message "Smoke me a kipper, I'll be back for breakfast - unfortunately some of your data won't". It then erased the contents of the hard disk.

The virus writer now faces 10 charges under the CMA (According to "Computing" 16 Feb., 1995).

3.7.2 Trojan Horse

The first Trojan Horses began in the US in the late '70s at a time when electronic bulletin boards became popular and it was possible to up- and down-load programs. It was discovered programs could be up-loaded that would alter all the files in the Bulletin Board. Thus the Trojan Horse was born. A Trojan Horse involves the unauthorised insertion of algorithms into a program which is then loaded onto a system causing illegitimate actions. Such actions could be to create a new account with privileges or obtain a password. The program may also allow easy access to an already penetrated system.

Trojan Horses differ from viruses in that they are a "parasite" and may not destroy the host but leave the system to continue functioning normally. Trojan Horses are still illicitly transferred into bulletin boards - sometimes erasing or scrambling files.

3.7.3 Worm

This term has been derived from "tapeworm" - a parasitic organism that lives inside a host and uses its resources to maintain itself. (SPAFFORD 1989). A worm is a program which runs independently and can relocate itself on another machine ("self- replicating").

Worms exist in memory and are non-permanent. They actively seek out idle machines, retreating when machine load increases. This distinguishes worms from viruses which, at present, have none of these capabilities.

The first worms were built and experimented with in 1979 - designed to travel from machine to machine to do useful work - not to break into systems. SHOCH and HUPP (1982) showed that worms could be usefully used as diagnostic tools for an Ethernet installation.

The "Internet Worm", as it has come to be known, attacked the system using password cracking and by overstacking data into a status report function - all done without attracting notice - thus resembling legitimate code. After infection the worm replicated itself and moved to another system.

3.7.4 Trapdoor

This attack involves insertion of clandestine code that will allow future unauthorised entry to a system without fear of discovery. An example is hidden code which will open a comms. channel unbeknown to the legitimate users of the system.

3.7.5 Logic and Time Bombs

A logic bomb is a piece of illicit software activated by a

specific combination of computer processes. For example the legitimate request for a payroll program to run may subsequently trigger execution of illegal activities. Time bombs are activated by the computer's internal clock.

3.8 Deception

In the Law Commission's working paper on Computer Misuse (HMSO 1988), it was recommended that intentional deception of a computer system should be covered by criminal law. Now covered under the Computer Misuse Act, 1990, the culprit would be securing unauthorised access by pretending to be another user.

No further explanation is given here. Copies of these reports can be obtained by E-mailing minniear@cs.purdue.edu and requesting number 823 and 933.

3.9 Hardware Theft

Theft of *software* is generally seen as unauthorised copying however floppy disks can be stolen. In 1984 the Waterford Glass Company had 25 disks stolen which held unique instructions for their glass cutting machines. Computerised mailing lists are easy targets and can change hands for considerable sums of money.

Hardware theft - stealing the actual computer - is fast becoming another crime against businesses and educational "soft targets".

Recently, a number of thefts have taken place against the Apple Macintosh computer. "Apple Mac" equipment is used by newspapers, graphic designers and publishers and is small, light and extremely valuable with expensive add-ons such as scanners. The Independent reported on 5th June, 1994 that hardware thieves are costing the Industry over £100m every year.

3.10 Pornography

This is the newest form of computer abuse criminals attempting to sell pornographic material are aiming it at the ever increasing PC- literate teenager market. What would you do if you found files called "Slowly.dl" or "Twice.gif"? Pornographic images stored on computer would seem no more explicit than those in books and magazines. The main difference is the medium on which pornography is stored and distributed.

There has been much publicity recently concerning computer pornography and the Government has approved an investigation by a Home Affairs Committee. These factors suggest this new trend in IT is gradually being adopted by the compilers and viewers of pornography.

Floppy disks and CD ROM's are cheap, easy to copy, do not deteriorate and are easily portable. CD ROM's have 600 times greater storage than floppy disks and high quality complex moving graphics can be stored. They also allow privacy by passwording and encryption.

Growing evidence supports computer pornography is appearing in school playgrounds where disks can be bought for as little as £1 and carry images copied from photographs, videos and movies

4.0 Types of Criminal

Who are these people? MITCHELL (1994) suggests a certain proportion of people are always honest and, if presented with the perfect crime, would turn it down. Conversely, others are so dishonest they would attempt to subvert the most secure of systems. The remainder are only as honest as the system under which they work. Distinctions are made between employees using company computers for personal work, (to which the employer may turn a blind eye) and "professionals" who make a living out of misusing computer facilities.

HUTT, BOSWORTH & HOYT (1988) see computer related crime as an iterative process involving the MOMMs concept - Motivations, Opportunities, Means and Methods:

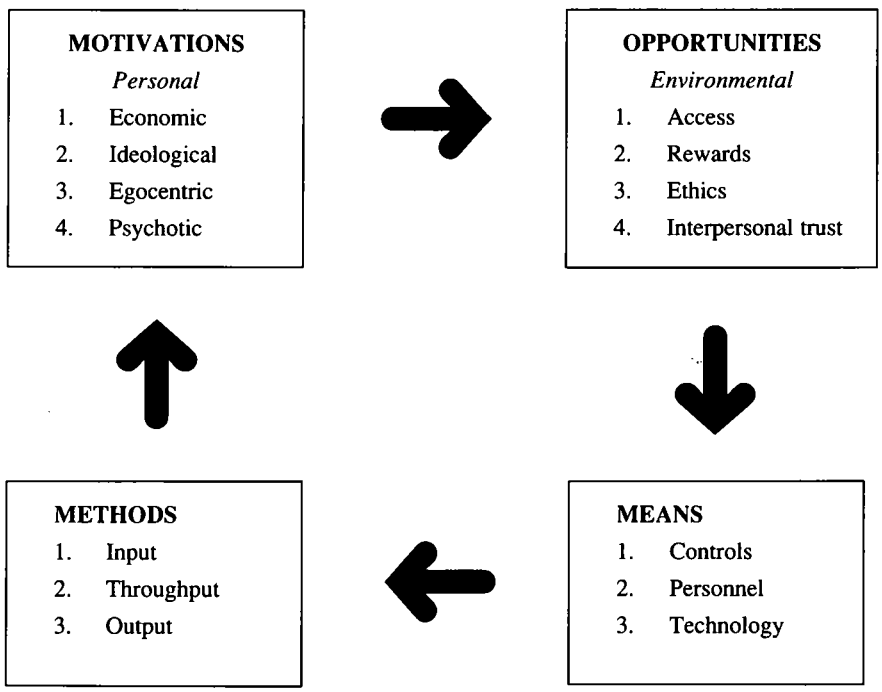

Figure 1.0 MOMMs - analysis of computer related crime

There seem to be many attempts to classify the criminal into a specific type for the crime committed. There is a commonly held view that a typical computer criminal is something of a "whiz-kid" with highly developed computing skills and a desire to "beat the system". Many exhibit opportunistic phenomena - exploiting weaknesses in the system being used which would solve pressing financial problems. Others tend to be relatively honest and in a position of trust who do not consider their abuse to be truly dishonest.

Crimes involving sabotage are often based on employees feeling frustrated or dissatisfied with aspects of their job. Computer abuse often appears "soft" and not viewed as a criminal act. Shuffling numbers around is not seen the same as handling gold bars or stealing huge sums of money; copying software does not physically leave the victims devoid of their possessions.

The following describes those in society today who attempt to commit computer abuse/crime:

4.1 Fraudster

Fraudsters are usually long-term employees in positions of trust, working long hours and not taking holidays - "the perfect employee" - which could of course give rise to suspicions.

BENBOW (1992) identifies five types of fraudster with associated examples:

The Opportunist
Having the ability and knowledge to manipulate accounts.

The Habitual Claimant
Using many different names - even countries - to commit fraud time and time again.

The Patient Claimant
Perpetrating the same fraud time and time again.

The Providers
Large volumes of transactions by service providers can easily be committed.

The Organised Gang
Large organised gangs running complex frauds.

MEALL (1993) in an article "Fraudsters with a Future" in the May edition of *Accountancy* concludes that the computer-literate fraudster has a bright future.

4.2 Hackers

Hackers love computers and have developed the expertise to use them in very clever ways. They circulate newsletters, attend trade shows and even have their own "conferences" such as the Chaos Computer Club where demonstrations are held and techniques exchanged.

Most hackers are school or college students. In Dorothy Denning's report on hackers (DENNING 1990) it seems most are more comfortable behind a computer screen and of unknown identity rather than interacting socially. Denning's initial findings suggested "hackers are learners and explorers who want to help rather than cause damage and who often have very high standards of behaviour". JOHNSON (1994) would dispute Denning's view as she suggests it is clear that people have been harmed by hacking.

Recently hacking has acquired a new connotation - "cracker" - which refers to those who use computers for illegal, unauthorised or disruptive activities. STOLL (1989 in "The Cuckoo's Egg") makes it clear that hackers pose a real threat to the security of nations. High-tech spying is becoming commonplace and hackers are being actively recruited.

4.3 Curious Intruders

Although well-intentioned, these types still recklessly cause damage to computer systems. According to Robert Morris (of the Internet Worm) he never intended to do such massive damage but he caused widespread havoc, crippling over 6000 machines and inconveniencing hundreds of users. Even an intruder who merely browses through a user's files is violating the privacy rights of that user. If any outsider entered a company office and began reading files in a cabinet there is no doubt they would be trespassing. Is there any basis for treating a trespasser who accesses information from a computer any differently?

4.4 Saboteurs

Disgruntled employees who wish to do harm to the company for revenge. Additionally, simply hating the job or sabotaging for fun - for example causing stock market plunges by pressing various phone buttons just because of the enjoyment of "scrambling things on the trading floor" (SPROUSE 1993).

5.0 Computer Misuse Act, 1990

On 29th June, 1990 the Computer Misuse Act became law. The Act defines three offences:-

- **Unauthorised Access Offence**
- **Ulterior Intent Offence**
- **Unauthorised Modification Offence**

5.1 Unauthorised Access Offence

This offence was defined partly to deter hacking but also to deter authorised users who decide to exceed their authority. Thus, hacking was criminalised. Section 1(1) of the Act reads:

A person is guilty of an offence if:

a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

b) the access he intends to secure is unauthorised;

c) he knows at the time that he causes the access that this is the case.

Section 1(2) removes many possible excuses from the offender:

The intent a person has to have to commit an offence need not be directed at:

a) any particular program or data;

b) a program or data of any particular kind;

c) a program or data held in any particular computer.

The offence lies in causing the computer in question to perform any function with the *deliberate intent* to secure access to programs or data held in the computer and knowing that this access is unauthorised. Thus hacking can be said to be "covered" - from simply reaching a main menu to completely roaming around the system.

5.2 Ulterior Intent Offence

This is viewed more seriously by the Act if the unauthorised access already gained is used to further some more serious crime. Thus, Section 2(1) of the Act reads:

A person is guilty of an offence under this Section if he commits ... the unauthorised access offence with intent to:

a) commit an offence .... ;

b) facilitate the commission of .... an offence (whether by himself or by some other person).

The offence involves unauthorised access to a computer system with the intention to carry out or facilitate the commission of a further serious crime. The important factor is the intention to commit the subsequent offence, whether or not it is possible.

5.3 Unauthorised Modification Offence

Section 3(1) reads:

A person is guilty of an offence if:

a) he does any act which causes an unauthorised modification of the contents of any computer; and

b) at the time when he does the act he has the requisite intent and the requisite knowledge.

The "knowledge" being if he knows he is unauthorised to carry out the change(s) which he effects. The "requisite intent" must be malicious.

This offence covers a wide variety of activities such as erasure and/or modification of data; planting of logic bombs, worms and viruses; preventing an authorised user gaining access. Thus only the intent to impair is sufficient for prosecution even if the damage had been done at once or will be done at some time in the future.

As noted by Wendy LONDON (1992), the definition of computer crime and abuse is conspicuous by its absence.

According to a DTI report there is still poor awareness of the CMA itself and risks associated with computer misuse. Indeed, some respondents to the survey had not seen or read the Act. There was however recognition that the aim of the Act was to deter computer misuse.

There was widespread belief that, should a case arise where prosecution was a possibility, many firms saw few incentives in pursuing the case as any results would be of modest benefit should the prosecution be successful. Doubts over direct benefits to the company were presented. Unlike civil cases, criminal cases prosecuted under the CMA will provide no restitutional benefit such as compensation.

There have only been a few cases to date, companies preferring to carry out internal investigations instead. The first case of hacking to be heard under the CMA was on 17th March, 1993 over two and a half years after the act came into force. Three students (Bedworth, Woods and Strickland) were charged with conspiracy. The latter two pleaded guilty and each received a six month jail sentence. The former was acquitted after pleading not guilty. Had he been charged with hacking *per se*, he may have been convicted.

6.0 Hackers for Hire

Sometimes one of the best ways to protect your systems is to break into it. It is perfectly legal to hire someone to break into your own computer and communications systems and explore system weaknesses.

Hiring hackers is a new countermeasure - one which causes some companies to shudder at the thought - but is a good way to see how vulnerable your system really is. Hackers often confirm corporate doubts and find new weak links. Even large companies are now "getting in on the act". Price Waterhouse has begun to offer hacker-like "penetration services" to clients.

Incidents are described by Ian Murphy, or "Captain Zap" who was reported in HUTT, BOSWORTH and HOYT (1988) as gaining unlawful access to a database containing nearly 2,000 Visa account numbers and ordering over US$350,000 worth of computer hardware. Murphy was fined US$1,000 and given 3 years probation, 1500 hours community service and his personal computer system was confiscated. Eleven years later he appeared in Information Week (VIOLINO 1993) claiming to make over US$500,000 a year for his services!

There is inevitably a conflict here of wanting the best for your systems but needing to hire these types as they are seen as "the elite". Some organisations feel it necessary to hire hackers - "the last line of defence". Captain Zap summarises thus after a company, who suspected they were being hacked hired him: "They had to go to somebody and they don't trust anybody now. Except me."

7.0 Federation Against Software Theft

The pace of technology has now provided the means for software distribution on a wide scale leading to the mass-production of seemingly legitimate products is ever increasing. This has lead to the innocent purchasers being duped into believing they are buying original and legitimate software when all they are getting is pirated versions.

FAST's Anti-Piracy Unit aims to expose organised networks of software thieves who have been exploiting mass software copying. Up to £120,000 worth of current but illegal copies of leading business software has been seized on CDs alone. FAST has also managed to seize software not yet available in the UK by linking up with the USA.

FAST's increasing power lead to the prosecution of a UK home-based counterfeiting operation involved in packing illegal disks and such authentic-looking sets of documentation that many software industry members were fooled. A sentence of six months imprisonment and payment of court costs of £5,000 were secured.

Much software is "stolen" from within - companies copying their already paid for programs onto more computers than their licences allow.

FAST is attempting to educate the small office and home-based office (SoHo) to ensure awareness of the law on software copying. It was found many people do not realise they are committing an offence by making copies of software for home use or "sharing" copies around the office.

FAST sees itself as being needed today more than ever as opportunities for software theft increase. It highlights a positive shift in attitudes amongst court judges as an unrivalled success and a promising step towards reliable accounting of software

usage. In early 1995, the organisation issued guidelines on how to quantify and monitor software assets. It now states no one should consider themselves immune from the law.

FAST Ltd
1 Kingfisher Court
Farnham Road, Slough
Berks SL2 1JF
Tel: 01753 527999

FAST has teamed up with the Business Software Alliance (BSA) to jointly manage "Operation Software Crimeline" which encourages employees to expose illegal software use by companies.

Business Software Alliance

The Business Software Alliance (BSA) is a world-wide organisation aiming to eradicate software piracy. With programs in more than 60 countries the BSA claims to implement effective anti-piracy programs. Members include Lotus Development, Microsoft, Novell and the Santa Cruz Operation.

Since inception in 1988 the BSA has brought 500+ legal actions against organisations who have violated software copyright laws. These include abuses from loading illegal software onto computers before shipping, to organisations making copies for their own internal use.

When settling legal actions against software copyright infringements, the BSA seeks:

- erasure of illegally copied software and replacement by purchase of legitimate software;

- compensation for damages and legal fees;

- a public statement by the company expressing its commitment to comply with the copyright law in future.

Recently the BSA took successful legal action against a German company who were using illegal copies of software. BSA worked with the Swedish police who subsequently raided five computer hardware dealers who had been copying hundreds of Microsoft products. This then lead the Czech police to raid an aircraft manufacturer, finding over 180 suspected illegal software products from Adobe, Novell, Lotus and others.

Even in China raids have been conducted and the BSA estimates that software piracy in that country cost the Industry US$595.9 million in 1993.

Figures quoted by the BSA for piracy estimates in 1993 are shocking:

Country	Piracy rate	Revenue Lost (US$)
Germany	57%	1,584,104,466
People's Republic of China	94%	595,881,900
Peru	98%	25,033,500
Russian Federation	98%	75,460,000
United States	35%	2,253,286,870

Country	% Worldwide Total	Total Revenue Lost
Africa/Middle East/India	5%	666,440,105
Asia	31%	3,963,527,364
Europe	38%	4,900,882,960
Latin America	7%	821,992,751
USA/Canada	19%	2,487,360,944
Worldwide Total		**US$12,840,204,124**

Business Software Alliance
First Floor,
Leconfield House
Curzon Street
London
W1Y 8AS
Tel: 0171 491 1974
Fax: 0171 495 3101

8.0 Useful Contacts

The authors feel that computer abuse is such an important topic in the commercial world of business that they have included some useful contact points which are current at the date of writing.

8.1 The Data Protection Act, 1984

A substantial information pack can be obtained from:-

The Office of the Data Protection Registrar
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Tel: 01625 535777
Fax: 01625 524510

8.2 Computer Crime Unit

This unit of the Metropolitan Police principally deals with offences where the computer itself is the object of the attack. More information can be obtained from :-

Tel: 0171 230 1177 (D.I. John Austen)

8.3 European Leisure Software Protection Association (ELSPA)

ELSPA has been set up by the £1bn games industry to deal with illegal copying of computer and video games. Recently it has smashed a million-dollar-a-week credit card fraud involving AT&T in America (Computing, 16 February, 1995). More information can be obtained from:

Tel: 01386 830642

SUMMARY

There is a general awareness in the commercial world that computer abuse is widespread. It is hoped that this paper has highlighted the following points :-

- Computer abuse is probably far more widespread than anyone cares to admit.
- Fraud is the most common commercial computer abuse.
- There is no such thing as an innocent hacker.
- Most computer systems are susceptible to attacks on their software because of the volumes of software exchanged between users.

It is also hoped that this article has been informative and left the reader with some substance about computer abuse.

- The four main categories of criminal are :-
  - fraudster
  - hacker
  - curious intruder
  - saboteur.
- The CMA (1990) defines three offences :-
  - Unauthorised Access Offence
  - Ulterior Intent Offence
  - Unauthorised Modification Offence.
- Help is at hand from organisations such as FAST and BSA.

Bibliography

Benbow, G. (1992) "The Criminal Element", *Computer Control Quarterly*, Vol. 10, Issue 4, pp 19-21.

Denning, D.E. (1990) "Concerning Hackers who break into Computer Systems", *Proceedings on 13th National Computer Security Conference*, 1-4 October, Vol. 2, Issue 13, pp 653-663.

FAST "Information Pack, Software use - Code of Conduct".

FAST (1994) "Audit Pack", pp 1.

Forester, T. & Morrison, P. (1990) "Computer Ethics - Cautionary Tales and Ethical Dilemmas in Computing", Oxford, Blackwell.

Hutt, A., Bosworth, S., & Hoyt, D. (1988) "Computer Security Handbook", McMillan, New York, pp 60-61, 253-254.

Johnson, D.G. (1994) Excerpt from "Computer Ethics" Prentice Hall, USA, 1994, *Educom Review*, Sept/Oct 1994, pp 47.

London, W. (1992) "Computer Crime: Law and Regulation - Protection and Prosecution", Cameron Markby Hewitt, London, pp 9.

Meall, L. (1993) "Fraudsters with a Future", *Accountancy*, May 1993, pp 74.

Mitchell, J. (1992) "Computer Audit - The Youngest Profession", *Computer Bulletin*, February/March,1992, pp 9.

Mitchell, J.A. (1994) "Computer Abuse", *Little Heath Services*, pp 7.

Shoch, J., & Hupp, J. (1982) "The Worm Programs - Early experiences with a distributed computation", *Communications of the ACM*, Vol. 25, No. 3, pp 172-180.

Sizer, R. (1994) "Security Guidelines in IT for the Professional Practitioner", *Computer Law and Security Report*, Special Supplement, Elsevier Science Ltd, pp 1 - 23.

Spafford, E. H. (1989) "The Internet Worm Incident", Purdue University, Nov, 1989, pp 3.

Sprouse, M. (1993) Excerpts from "Sabotage in the Workplace", Pressure Drop Press, *Information Week*, USA, March 8, 1993, Issue 415, pp 34-42.

Stoll, C. (1989) "The Cuckoo's Egg", Simon & Schuster, USA.

Violino, B. (1993) "Hackers for Hire", *Information Week*, USA, Issue 430, June 21, 1993, pp 52.

No author (1989) "Viruses, worms et al", *Software World*, Vol. 20, No. 3, pp 13. Computing, 13th October, 1994.

Home and Away

M. Herrison

(The saga continues. Monsieur Herrison, having heard that he has been awarded a bottle of the bubbly stuff for his previous efforts, has now worked out how he can obtain said item without revealing his identity. This involves your editor making a short trip to France at your expense!)

'Ello, ello, mais amis,

Again into the fray our intrepid (now experienced) international auditors have visited the French subsidiary. This time no more at the head office but out into the field at an operational unit. (operational maybe too strong a word, remote site might be better).

Well let me begin.

One mercredi (Wednesday to you) morning, once again I set sail from Dover alone, mes colleagues already being a la France. One thirsty hour and a bit later (I don't know why I keep taking the ferry when I have to drive at the other end. I sit for an hour and a bit looking at a busy bar selling beer at duty free prices, often surrounded by drunks and having to abstain!) Anyway where was I? Oh yes, Calais.

Now these frenchies do know a thing or two about building roads. Once you clear their customs and passport control straight onto fast and relatively clear roads. Slight prob, le peage. I always get behind a non french person (no not always British, in fact usually Belgian) who hasn't got the wherewithal to pay, which then results in half a dozen cars two caravans and a truck having to reverse 50 yards (sorry metres).

Back on the move again, this time on smaller roads, 2CVs and tractors. Road rage here is still not a major problem possibly due to the size of ditches at the side of the road.

Et enfin l'hotel. This semain another old chateau type, pretty gardens, comfortable rooms, gourmet restaurant and astronomic prices. But where are les colleagues? Pas ici I have forgotten the euro hour and it's later than I thought and they've deserted moi. Helas. There is nothing for it but to eat alone and hit the bottle. As someone else once said 'tomorrow is another day'.

Le matin... of course now it's an hour earlier than my brain thinks it is, not to mention liver and kidneys.

Le petit dejeuner. Petit is the right word £7.50 for a cup of coffee and three pieces of bread one plain, one croissant and pain au chocolat (is that like death by chocolate but not so bad?). This is not enough to soak up the previous night nor to keep body and mind together.

And so to work:-

We are going to a unit in the middle of nowhere. It was a mining town once but just like Barnsley and south Wales the only use for the old black stuff now is for bar-be-ques = no wealth = no spend = no profit. We intend today to make introductions and spell out our plan for forthcoming couple of days and following week. Initially we'll observe procedures so we can document, test for controls and other audity things later. C'est facile, there are no controls. This however, is not a major weakness as there are no customers either and the few that are there have the social service department invoiced for their purchases.

On to other areas, plus important areas I might add, lunch. Today a small inn in a nearby town. Well the beer was ok but I still don't know what we ate. Le soir. A previously unexplored restaurant with langustines on menu. Now I know they are safe here. Wrong again.....I am going to stick to horse.

I know says I (well travelled chap that I am) let's stay in a city next week. Where we will be working is near Lille. Let's stay there. Pin in le vieux Michelin and bobs votre oncle.

Lundi matin by shuttle this time with colleague who doesn't appreciate the finer points of a P & O cruise and for the first time get stopped by le security. 'It's him. He looks like a terrorist'. Quick chat with the security leader who doesn't even bother to look in back of car. We have only been stopped due to getting stroppy with p**t at ticket kiosk who has called ahead that we look sus.

Now a bon thing about going to Lille, the autoroute is not a peage... c'est gratuit. Find (eventually) hotel in centre of city. Car park is entered on the wrong side of a no through road one way street. There is only one way and that is a U turn across a no U turns central reservation. Bizarre.

This place is OK. Mini bar, Financial Times and lots of bars and restaurants in town, weather warm (il fait beau) and all les girls in short jupes (or tight shorts). Now remember nous etes en France, so we look for a Chinese! Yup there are a few (also spot an Indian Le Maharajah). But it is warm....leave windows open all night. Next day we have all been bitten by bugs various.

Oh well. Back to work things. Now this trading unit takes (or could if proffered) foreign currency. What is le regule re change or coins Je demande. (why does coin mean corner). No prob came le reponse. Oh and how is it banked? Ah a problem. So what do you do with it? (There is a stock pile of foreign coinage in safe) !!!

Lunch a nice looking pizzeria called (AUX LES DEUX MAGGOTS). Oh well, we were hungry. Now I'm not so sure. The week progressed, we tried le Indian, a tandoori no less. Speciality of the house too Tandoori Quail! This was a strange experience as it is probably the first meal out we had which didn't have an after effect.

One soir we met with some of our French colleagues. We visited a bar that was a brewery which brewed 'real ale' well as near as you are going to get in France. Half litre a glass, a mere 4.00FF a shot. After half a dozen (6% strength) it all seemed like a good idea.

And finally back to blighty for R & R.

Another Monday and here I am back in small hotel used earlier in the year. Hot day and lessons learned from previous visits. I have brought my own sparkling water to drink if thirsty in night. Unpack bag, change clothes, put two bottles in sink, plug in, add water. Then promptly forgot all about it. Went down for couple in the bar, then around le town. After several pit stops return to hotel. No bar staff, no receptioniste, Odd! Go upstairs. Oh b***s!! On floor there is the entire hotel staff including chef (in his cheffing gear) on hands and knees mopping the carpet. I have flooded l'hotel. I am so embarrasee that I join in... an hour or so later most of mess cleared but now entire floor smells

damp. There are towels everywhere. Yet another place where I can't show my face again.

Now this trip..found a new **** hotel to eat at (Michelin recommended) Tres bon.... partook of the 170FF menu starter, some sort of fish dish.... didn't know what, but had it anyway... Not bad... All in all great meal... Back home discovered it was Scorpion Fish. Glad I hadn't known that.

Nice place though, a mere £90 for the two of us (cheapest vino wasn't very).

Well all that was a couple of weeks ago, et je suis going en vacances anyday now maybe I'll recover enough to rejoin le fray peut etre.... Je pense je vous emette un carte poste pendant la vacance.

Salut.

M.Herrison.

Book Review

John Silltow

Title: **Java Sourcebook**

Author: Ed Anuff

Publisher: John Wiley & Sons

ISBN: 0-471-14859-8

Pages: 498

Price: £19.99

Reviewer: John Silltow,
Security Control and Audit Limited.

Java is a simple object-oriented language that has many elements in common with C and C++, but has also removed or streamlined the areas where many programmers have had difficulty or that have been the most frequent sources of bugs. Java is also a intended to be a secure language, making it possible to restrict the access of Java programs to parts of the system, such as files and memory address, without limiting the language capabilities.

This book is a good introduction to the subject and is organised into four parts:

- how to get and install the Java Development Kit,
- the nuts and bolts of the Java language,
- building HotJava applets, and
- available reference material.

It should be explained at this point that whilst Java is the language, HotJava is a specific application. It is in fact Sun's Web browser.

As Java is a language of the Internet, it is necessary to have a connection to obtain the source code and updates. The Java Development Kit can be downloaded for UNIX, Windows '95/NT and the Macintosh platforms with other options becoming available according to demand.

It is nice to see a section on security within a programming manual. There is some concern currently that Java applets can in fact be corrupted and actually create security exposures but as this knowledge has only recently emerged, this book should not be faulted for not alerting its readers to the potential problem. Elsewhere, it does raise issues and drawbacks with the language wherever they appear and provides an open discussion on the options.

The main purpose of this book is to teach Java programming. It does that admirably in the 350 pages devoted to that aspect. It includes all the coding instructions for handling full multimedia applications as well as creating applications which can be ported to other platforms. There are a further 100 pages of appendices devoted to working examples.

This book is an incredibly easy read. The style flows well and it is easy to forget it is a tutorial. I came to it in order to understand the language from a security point of view and have now picked up the urge to learn more and create a few applications of my own. I cannot provide a better testimony for it.

★ ★ ★ (Highly recommended)

Eurospeak

(One of the many problems faced by the auditor is the need to communicate clearly via the written word, especially where the subject may be of a technical nature and the likely audience will be of a varied nature. To help solve this conundrum I provide the following guide to international communication as recently issued in a draft discussion document by the European Union - Ed.)

Having chosen English as the preferred language in the EEC (now officially the European Union, or EU), the European Parliament has commissioned a feasibility study in ways of improving efficiency in communications between Government departments.

European officials have often pointed out that English spelling is unnecessarily difficult; for example: cough, plough, rough, through and thorough. What is clearly needed is a phased programme of changes to iron out these anomalies. The programme would, of course, be administered by a committee staff at top level by participating nations.

In the first year, for example, the committee would suggest using 's' instead of the soft 'c'. Sertainly, sivil servants in all sities would resieve this news with joy. Then the hard 'c' could be replaced by 'k' sinse both letters are pronounsed alike. Not only would this klear up konfusion in the minds of klerikal workers, but typewriters kould be made with one less letter.

There would be growing enthusiasm when in the sekond year, it was anounsed that the troublesome 'ph' would hense-forth be written 'f'. This would make words like 'fotograf' twenty persent shorter in print.

In the third year, publik akseptanse of the new spelling kan be expekted to reach the stage where more komplikated changes are possible. Governments would enkourage the removal of double letters which have always been a deterent to akurate speling.

We would al agre that the horible mes of silent 'e's in the languag is disgrasful. Therefor we kould drop thes and kontinu to read and writ as though nothing had hapend. By this tim it would be four years sins the skem began and peopl would be reseptive to steps sutsh as replasing 'th' by 'z'. Perhaps zen ze funktion of 'w' kould be taken on by 'v', vitsh is, after al, half a 'w'. Shortly after zis, ze unesesary 'o' kould be dropd from words kontaining'ou'. Similar arguments vud of kors be aplid to ozer kombinations of leters.

Kontinuing zis proses yer after yer, ve vud eventuli hav a reli sensibl riten styl. After tventi yers zer vud be no mor trubls or difikultis and evrivun vud fin it ezi tu understand ech ozer. Ze drems of ze guverment vud finali hav kum tru.

Whilst on the subject of clear communication, a statement taken from a young child's essay on maritime history does show just how important the correct choice of word can be in conveying the correct message. The statement read - *"Sir Francis Drake circumcised the world with a 100 foot clipper"*.

Overhead at the programming department's Christmas party. *"No I'm not worried about things getting out of hand, we all practice safe hex here"*.

ON BEING SIXTY

Although audit is often seen as a young person's game, I was particularly taken by the following poem which was written some twelve hundred years ago; probably as a result of my own advancing years! - Ed.

Between thirty and forty, one is distracted by the Five Lusts; Between seventy and eighty, one is a prey to a hundred diseases; But from fifty to sixty one is free from all ills; Calm and still - the heart enjoys rest; I have put behind me Love and Greed; I have done with Profit and Fame; I am still short of illness and decay and far from decrepit age. Strength of limb I still possess to seek the rivers and hills; Still my heart has spirit enough to listen to flutes and strings. At leisure I open new wine and taste several cups; Drunken I recall old poems and sing a whole volume. Menge-te has asked for a poem and herewith I exhort him not to complain of three-score, "the time of obedient ears".

Po Chu-I (772-846 A.D.)

Note: "the time of obedient years" refers to Confucious' statement that it was not till he was sixty that "his ears obeyed him". - Ed.

CASG MATTERS

REPORT FROM THE MONEY BOX

This column, dealing with the financial matters of the CASG, is prepared by ***Bill Barton*** *our Treasurer.*

We are only just into our new season and have still to have our first technical briefing session. Our financial results reflect income and expenditure for the first three months of the new financial year, to 31 July 1996.

Income to-date is £1,922, being £1,830 from the 1996/97 annual subscriptions and £92 from bank interest.

Expenditure has been £1,183 for the summer journal, £325 on costs for the technical briefing sessions and £244 on general administrative expenses. This totals £1,752.

This gives a profit to-date of £170.

Our objective for this year will be to break even. This will be dependent on attendance at the Technical Briefing sessions, so I urge all to support the Group and attend the first meeting on 8 October 1996 on Auditing and Automation at the Chartered Accountants' Hall in Moorgate Place, London. I am certain it will be a worthwhile event.

PEOPLE PROFILES

David M Judge

Current Position: Consultant, Emprise Technologies Europe

CASG Involvement: Journal Contributor

David Judge has been associated with the computer industry for 35 years, of which 26 were spent working for IBM in various roles. Having completed an apprenticeship in industrial electronics, and a year as a technical writer for EMI, David joined IBM in 1967 as a hardware engineer. He quickly transferred to software support in 1971 and was a support specialist on CICS/VS, DOS/VS, DL/1, PL/1 and COBOL/VS for several years before becoming a specialist on the 8100 programme with emphasis on DPPX. He then worked as a support specialist on a large supermarket account before transferring to internal IS support at IBM's headquarters in Portsmouth.

In 1986 he spent three years on assignment in Colorado, USA where he first became involved in BS5750 implementation. On his return to the UK much time was spent on process and workflow management products and he was responsible for several projects to implement these products into the

IBM Software House. Here again ensuring compliance of the projects and products to BS5750/ISO9000 was part of David's brief.

Having left IBM in 1992, he took a break from the IT industry, before returning to work for Emprise Technologies Europe as a technical consultant, supporting the various products the company develops and distributes, including **CATS** (**C**ICS **A**utomated **T**able **S**ystem).

He can be contacted at: Emprise Technologies Europe, Brue Business Park, Bason Bridge, Highbridge, Somerset, TA11 6HF. Tel: 01278 795404 Fax: 01278 759286 or Email: davidj@emprise-tech.co.uk .

Sub-Editor Wanted

I am looking for an additional sub-editor to manage a regular *Opinion* column in the Journal. The intention is to provide a forum for people in the industry to voice their opinions on topical, or not so topical, issues. This will require the column's editor to seek contributions from both within and outside the CASG membership. If you would like to try this unpaid, but rewarding job, then please give me a call. Alternatively, if you do not want the role, but wish to share something with your colleagues, or to simply let off steam, then send me a contribution instead. - Ed.

BCS MATTERS

Colin Thompson
Director of Member Services

BCS gets Engineering Council seal of approval

The Society has emerged from a detailed review by the Engineering Council with flying colours. This review, conducted over the past year, was part of a standard pattern of 5 yearly reviews to which all engineering institutions are subject. Following a final presentation in June, the Engineering Council has now confirmed that the nominated status of the Society has been confirmed for a further 5 years and that we are now "licensed" to undertake the full range of processing functions on behalf of the Council.

Licensing is a new concept for Engineering Institutions and came into effect with the creation of the new Engineering Council at the beginning of 1996. Essentially it means that, for approved institutions, decision making functions are fully delegated with the Engineering Council retaining a quality assurance role rather than, as previously, a detailed approval responsibility. Licences are granted function by function and the Society joins a very select band of institutions which have been granted licenses covering all functions.

Most readers will be familiar with the problems which businesses are likely to face at the start of the new millennium, as many of our computer systems fail to cope with the change from a 2 digit to a 4 digit year reference. For many, the impact is likely to be serious, particularly when coupled with the disruption which will result from the planned introduction of the Single European Currency on the same date, and there is an urgent need for action on the part of both the profession and Business Management.

To assist the process, the BCS has now published an information note which explains the problem, illustrates some of the ways in which it is likely to manifest itself, and suggests what action should now be taken. This information note is available on the BCS Home Pages (http://www.bcs.org.uk). Those not yet wired can obtain a copy (price £2.50 to cover P&P) from the Marketing Department at BCS HQ (telephone 01793 417424).

A BCS Consultancy Register

The issue of whether the BCS should publish a register of members practising as consultants has been debated for some time and was the subject of recent correspondence in the *Computer Bulletin*. The issue, is in relation to a general consultancy register, is a complex one and there are some significant legal and financial implications for the Society. In an endeavour to bring this particular debate to a conclusion, the Professional Issues Board has now set up a Task Group, under the chairmanship of Peter Barnes, to consider the matter and make policy recommendations.

And a BCS Security Register

Whatever the case for a general register, there is agreement on the need for registers covering specialist expertise and the Financial Operations Committee recently approved limited funding to enable the Professional Issues Board to set up a register of security specialists and to consider the case for a security specialism within the BCS Professional Membership.

The detailed ground rules for the security register have yet to be defined but it is likely that registration will be limited to BCS Professional Members and the new Companion grade. Further information will be included in the next edition of this newsletter, and, in the meantime, I should be very happy to hear from anyone interested in registration.

Computing

Nothing is more guaranteed to increase my morning post than problems with the delivery of the weekly newspaper, *Computing*. It is clear from the letters I receive, that the right to free delivery, irrespective of grade or employment status, is one of the most prized benefits of BCS Membership. Equally clearly, all has not been well with the distribution system over the past year and we have had a number of meetings recently with Senior Managers at the publishers, VNU, discussing ways in which we can ensure a more reliable supply for BCS Members.

The outcome of these meetings has been a very clear commitment from VNU to provide a reliable service for members, and this has been backed up by a number of improvements to the distribution system, together with the creation of a new telephone service dedicated to handling queries in respect of *Computing*. Members who wish to register or who are experiencing difficulties with deliveries should call 0171 316 9818.

It is early days to make a judgement, but my postbag has shown a marked drop in the number of letters related to problems with *Computing*.

A New Distinguished Fellow

Last month saw the award of a distinguished Fellowship to Tim Berners-Lee, the creator of the World Wide Web. Tim Joins a very select band of professionals who have been awarded the Society's highest honour; only 20 other distinguished Fellowships have been awarded since the Society was formed almost 40 years ago.

And Finally.....

Views are invited on the subject of Continuous Professional Development. The Society is currently undertaking a review of its CPD scheme with a view to ensuring that it meets members needs and to bring it into line with the Engineering Council framework published in October 1994. As part of the consultation process, members are invited to submit views on any aspect of CPD to Malcolm Sillars, The BCS Director of Development. Malcolm can be contacted by post at BCS HQ, by Fax on 01793 480270 or by e-mail at msillars@bcs.org.uk. Views on any other issue covered in this article, or any other BCS related topic, should be addressed me, Colin Thompson, by post or Fax at the same address or by e-mail at cthompson@bcs.org.uk.

Library Services for BCS members

By Helen Crawford - BCS Librarian

The BCS library, which is held at the Institute for Electrical Engineers, is also available, free of charge, to members of BCS specialist groups. In this column, ***Helen Crawford****, the BCS Librarian, describes some of the publications available which are relevant to computer audit. If you wish to take advantage of this BCS service, then contact Helen at the address given at the bottom of the column. Ed.*

Since my last column, the BCS library has received and added to its book stock many new titles which are of extreme interest to CASG journal readers. In particular we have received a number of books upon the subject of computer security, which includes security and the internet. Other subjects of interest to readers are Systems Development, Disaster Recovery, and Computer Crime.

The BCS Library holds a number of computer Security journals in its stock. These include titles such as: Computer Fraud and Security, Computers and Security, Computers and Law.

To search our library stock it is now possible to contact us via the Internet, which is proving to be very handy to BCS/IEE members, as this means they no longer have to come into the library and search on-line. The library catalogue can be found at the following address:

http://www.iee.org.uk/Library/Catalogue/Simple-search.html

Once you have a selected a book you wish to see on loan then you can send an E-mail to the Library asking for the book to be issued to you and sent out. Easy!

Unfortunately our Journals catalogue is not available to search as yet on the Internet, but will be in the near future.

Copies of articles which are required can be obtained from our document supply librarian at the BCS/IEE Library at a cost. Please include a full bibliographic reference, so that they may find the particular article required quickly.

Lastly, here is a list of all the new books which are now available to borrow or look at within the BCS/IEE Library stock:

ISBN: 1-56592-148-8
GARFINKEL S, SPAFFORD G.
Practical UNIX and Internet Security
O+Reilly and Associates, 1996

ISBN: 1-56276-422-5
AMOROSO E, SHARP R
PC Week, Intranet and Internet firewall strategies.
Ziff-Davis, 1996

ISBN: 1-56205-545-3
STEEN W, BIERER D
Netware Security
New Riders Press, 1996

ISBN: 1-56884-457-3
VACCA J
Internet Security secrets
IDG Books Worldwide, 1996

ISBN:0-07-709082-9
HARGRAVE D
SSADM 4+ for rapid systems development.
McGraw-Hill, 1996

ISBN: 0-471-12175-4
OIGO J W
Disaster recovery planning: for computers and communication resources.
Wiley, 1996

ISBN: 1-87-466-32-2
DATA PROTECTION REGISTRAR
Our answers: Data Protection and the EU directive 95/46/EC
Data Protection Registra, 1996

INSTITUTION OF ELECTRICAL ENGINEERS, IEE COLOQ DIGEST 1996/151
Information Security- is it safe? Colloquium London, 27 June 1996
IEE, 1996

ISBN: 0-471-14160-7
ELLSWORTH J H, ELLSWORTH M V
New Internet business book
Wiley, 2nd Edition, 1996

ISBN: 1-56884-457-3
VACCA J
Internet Security Secrets
IDG Books World-wide, 1996

BRITISH COMPUTER SOCIETY
BCS position paper on key issues: EU directive on data protection.
BCS, 1996

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

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

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

British
Computer
Society

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

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:

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

casg
Computer Audit Specialist Group

British Computer Society

Management Committee

CHAIRMAN	Alison Webb	Consultant	01223 461316
SECRETARY	Raghu Iyer	KPMG	0171 311 6023 Email: raghu.iyer@kpmg.mark400.gb
TREASURER	Bill Barton	BSkyB	0171 705 6821
MEMBERSHIP SECRETARY	Jenny Broadbent	Cambridgeshire County Council	01223 317256 Email: Jenny.Broadbent@finance.cambscnty.gov.uk
JOURNAL EDITOR	John Mitchell	LHS - The Business Control Consultancy	01707 851454 Email: jmitchell@lhs.win-uk.net
SECURITY COMMITTEE LIAISON	John Bevan	Audit & Computer Security Services	01992 582439
TECHNICAL BOARD LIAISON	Geoff Wilson	Consultant	01962 733049
	Allen Brown	Consultant	01803 327874
TECHNICAL BRIEFINGS	Diane Skinner	Audit Commission	01179 236757
	Stan Dormer	Consultant	01565 634609
	Dave Cox	Lombard North Central plc	01737 774111
	Paul Plane	National Westminster Bank plc	0171 726 1000

Membership Enquiries to:

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

Tel: 01223 317256

Guidelines for Potential Authors

Types of Article

The Journal publishes many different 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.See below for details of the preferred format for refereed submissions.

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.

Academic Articles

All would-be authors should follow the Harvard system of bibliographic references. At the end of your article list all the references in alphabetical order. Always start with the author's SURNAME followed by initials ALLAN G.W. Then put the year of publication in round brackets ALLAN G.W. (1994) Next comes the title of the article which is put in quote marks ALLAN G.W. (1994) "This is the Title of the Article" Next print the title of the book/journal/periodical magazine in which the article was published. This should be in italics ALLAN G.W. (1994) "This is the Title of the Article" *This is the Title of the Periodical.* Then follows the Volume Number and Issue Number ALLAN G.W. (1994) "This is the Title of the Article" *This is the Title of the Periodical* Vol. 12 (3).

Submissions

All submissions should either be on double spaced, single-sided A4 paper, or on PC format diskette in ASCII, Word for Windows or Ami Pro format, or via e-mail in 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

Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ