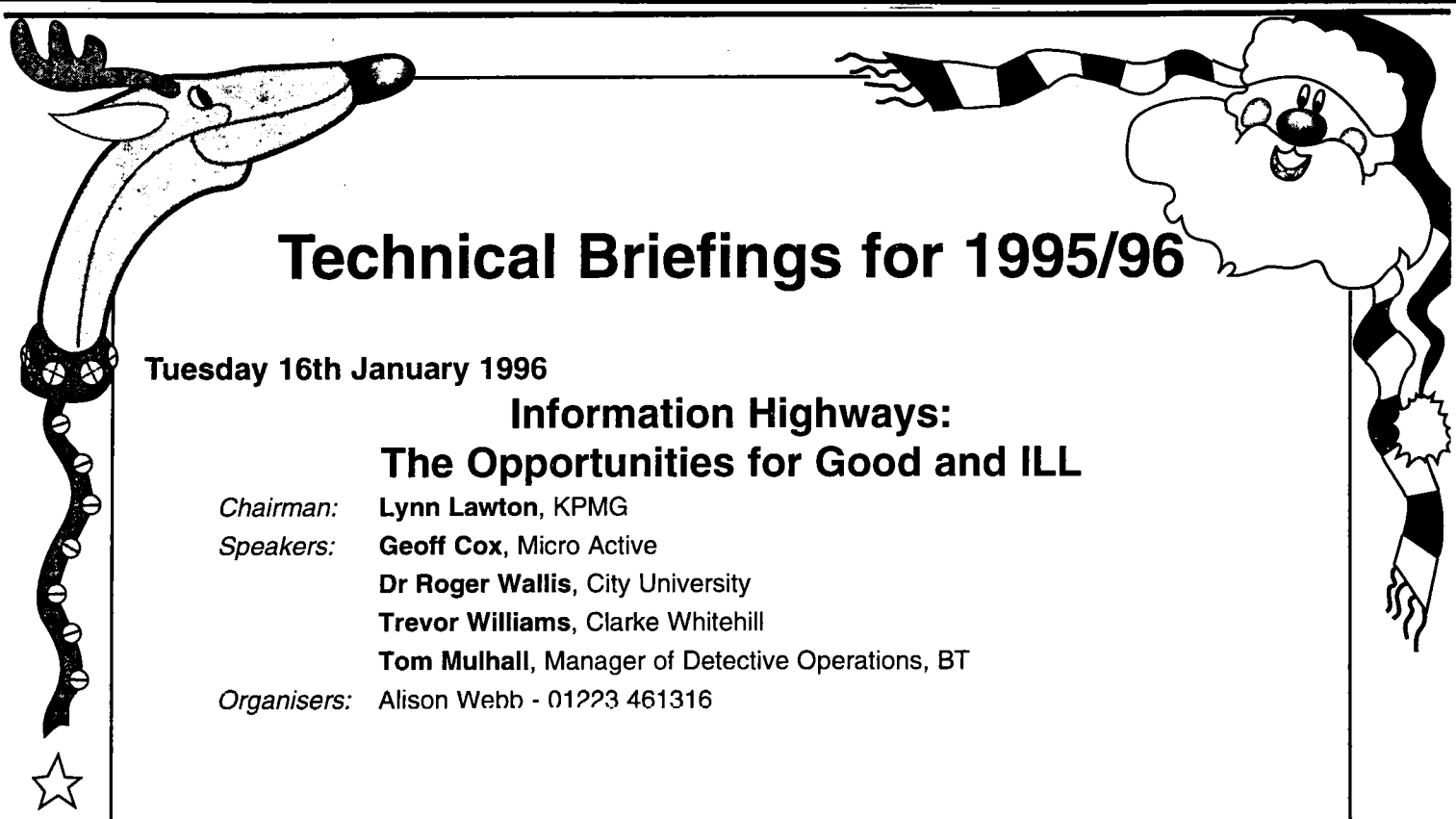
ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 6 NUMBER 3 WINTER 95

The British Computer Society



Technical Briefings for 1995/96

Tuesday 16th January 1996

Information Highways: The Opportunities for Good and ILL

Chairman: **Lynn Lawton**, KPMG

Speakers: **Geoff Cox**, Micro Active

Dr Roger Wallis, City University

Trevor Williams, Clarke Whitehill

Tom Mulhall, Manager of Detective Operations, BT

Organisers: Alison Webb - 01223 461316

Tuesday 16th April 1996

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

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

Speakers: **Graham Clukas**, Price Waterhouse

John Ford, Quality Methods Manager (IT), Safeway Stores plc

Sue Mathews, Training by Design

Stan Dormer, System Security Ltd.

Organisers: John Bevan - 01992 582439

Diane Skinner - 0117 923 6757

Tuesday 16th April 1996 16.30

ANNUAL GENERAL MEETING

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

For last minute confirmation contact the relevant organisers.

SEASON'S GREETINGS

Contents of the Journal

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

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

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

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

EDITORIAL

The more I.S. Auditors that I meet, the more I become convinced that there is a huge gulf between those that follow the procedures and those that really get to grips with the things that need improving in their organisation. The difference between these two camps is not one of training, education, or even experience. It is more a tad of intuition, coupled with a triple measure of neck-sticking confidence.

This last component is often the most sadly lacking ingredient in many computer audit departments today, simply because they forget that the I.S. department is populated by human beings; well almost as human as us auditors, if that is representative of human-kind. Now human beings often get things wrong, but they are often loathe to admit it, so they become very defensive and play upon the weakness of the opposition, which in this case is likely to be a lack of detailed knowledge of the issue under discussion. We feel that it is wrong, we actually 'know' that it is wrong, but can we prove it in advance of it happening? Nowhere is this more prevalent than in the area of system development auditing.

Well, in this edition we have the second part of George Allan's excellent paper on software estimating. You really should consider setting up his equations in your favourite spreadsheet to help you to estimate the development time and cost of the latest project that you have been directed to audit. Even if the results reflect a large variance from what is currently in the project plan, you at least have the basis for a sensible discussion with the developers. And your results are backed-up by extensive research. What supports their estimates?

We also have a refereed paper by Andrew Hawker which deals with the longevity, or otherwise, of computer records. Something that should be of great interest to auditors and managers alike.

The Chairman's Corner raises the thorny problem of BS7799 accreditation and certification. This is a really important area for any qualified (CISA, or QiCa) computer auditor. Read carefully, what your Chairman has to say on this subject, especially the bit about accreditation. If we are not careful we are going to have another qualification forced upon us in the same way that only TickIT qualified auditors can audit ISO 9000 software developments.

Then there is a marvellous guide to the Internet by Alan Oliphant which provides a wealth of useful advice and plenty of contact addresses of audit interest. Helen Crawford's column, which deals with the BCS Library, lists a number of useful publications which can be loaned to members of the CASG. Remember, this is only one of the many benefits of membership. Finally, we have a communication from the Continent which shows that travelling hopefully is often better than actually arriving.

Enjoy this edition over the Christmas break. The season's greeting to all our members from the management committee in general and your editorial team in particular.

John Mitchell

Chairman's Corner

Alison Webb

The best handbook on computer security I've ever come across is the DTI publication 'A Code of Practice for Information Security Management' (1993). Its authors are modestly anonymous, but everyone I've spoken to agrees they've done a very good job.

Most people will know that their work has now been published as British Standard BS7799, and that the DTI is now considering a scheme for accredited certification, rather like the BS5750 certification, based on this standard.

Obviously, the nature of the certificate needs thinking about carefully. The DTI is suggesting that each organisation outlines the state of its controls in a brochure. This would list the controls it had decided to apply selected from the standard, and an assessment of how effective they were in practice. This assessment would be made using a standard questionnaire.

There are, of course, a lot of potential problems with this, which the DTI recognises: and they will be familiar, too, to anyone with teenage children who's forced to take an interest in our educational system: the two methods of assessment are exactly analogous.

First, you decide what modules you want to study: (or what controls you need to apply). Some options are more demanding although arguably more rewarding than others. Then you produce your evidence of study, (or implement your controls), and the results are assessed, either internally, or by an independent certifier. There has been much acrimonious discussion about the difficulties of objective educational assessment, and the same arguments hold good in the security field: because, as the DTI itself admits, many of the judgements involved are subjective. Any internal assessment cannot be wholly impartial: and people recognise this when they employ external consultants, who may not be any cleverer or more knowledgeable than their employers, but who at least look at the situation with fresh eyes. Although the DTI suggest self-certification as a low-cost option, in practice, as they say, it may well be 'indicative rather than conclusive'. We can all write good references for ourselves.

The other area of contention will be the certification process itself. This takes a snapshot of the position at the time of the assessment, based on a questionnaire. There would be some auditing, or moderating, of the answers to the questions, but it's not clear yet what this would be. Continuing the educational analogy, students are divided into two categories: those who enjoy the challenge of an examination, and do often better than predicted; and those who dislike the stress, and do worse. This is why the move educationally is towards continuous assessment as an expensive but fairer method more likely to represent the reality: and with security, the same holds true.

We joke about managers signing a year's payrolls the day before the auditors visit, because we all recognise that to be effective, people must not just write procedures but apply controls as they do their jobs consistently over long periods. Teachers are doing the continual assessment in schools: and they say that the increased administrative burden reduces their effectiveness in the classroom. Who will do it for the company, and how will we pay for it - reduced productivity or extra overhead?

We are left with the need to reconcile two unreconcilable facts: people want assurance that companies have effective security: the cost of providing proper assurance is prohibitive. Perhaps the first fact needs a bit more analysis. Who is it, exactly, that needs this assurance? The DTI talk about 'business partners', which itself is interesting, because the only assessment every company must have at the moment about the state of its internal controls is that in the external auditors' report which certifies the company's accounts. Although there have been some determined attempts to blame the auditors when third parties like business partners suffer when accounts later prove misleading, it's still clear that this audit report is primarily for the shareholders: that is, the owners of the company.

And are all business partners interested? When I buy a bar of soap from the chemist, the length of their passwords doesn't seem that relevant to my decision. I might be more interested if I were Boots, buying my stock of soap from a small specialist manufacturer, but even here, I'd be selective. I'd be concerned about any processes that might affect my supply: but not so much about those that affected whether or not I was invoiced promptly.

Perhaps we need to define who is likely to be interested in our security, and what their concerns will be. This would mean that if I needed certification (to get my contract with Boots), I could concentrate on a sub-set of controls. I don't mean these would be the only controls in the company: but the expensive process of writing the brochure and getting it certified would be small-scale, because the assessors would only need to look at some of the things I did.

The worst thing for those of us who already assess security would be if the BS7799 certification didn't work. If virtually everyone who tries for it, gets it, they will understandably consider themselves perfect, and above criticism by the auditors. If it's withheld until they've corrected the trivial errors picked out in a superficial review, they'll spend time on the equivalent of correcting their spelling mistakes, and not on improving security.

We all need to comment on BS7799. If you aren't doing so already via your own organisation, let us know what you think. The BCS is feeding comments to the DTI via its Security Committee, and we all have a right - as auditors, even a duty - to have our ideas represented.

Guidelines for Potential Authors

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.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication.

News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity.

Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission.

All submissions should either be on double spaced, single-sided A4 paper, or on PC format diskette in ASCII 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 photograph, or electronic image.

CASG Editorial Submission Deadlines

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

Using the Internet - A Guide for Auditors

Alan Oliphant

Introduction

This article is intended for the internal auditor who wishes to take the first steps to entering the world of on-line communication through the Internet. It seeks to take some of the mystery from the terms that you will see bandied about. It is not for the experts. The experts do not read about the technology any more. They use it to their own advantage.

Disclaimer

I am not an expert in the Internet. I have been playing with it for about a year and a half and I am learning about it all the time. Therefore, I apologise to those who know more than I do. This article is quite clearly aimed at those who have yet to dip their toes in the water.

Also, this article is insufficient to give you a real flavour of the Internet. I can only hope to whet the appetite. For those of you whose appetites are whetted, I hope you also go on line and find it to be of benefit; Also that you begin to use the resources available and contribute to the world-wide body of knowledge by offering your own views and expertise to others.

Scope

This article is designed to promote the use of the Internet by internal auditors, not to provide a list of all the dangers and traps that lurk along the way. This would take an entire article in itself. Although I mention some of the problems, I will not dwell on them.

What do I hope to cover?

- Firstly some statistics about the Internet and some background on the different levels of connectivity.
- Secondly, those facilities which are of use. In particular:
  - Electronic mail
  - The use of Listservers
  - The Usenet newsgroups
  - File Transfer
  - Archie and Gopher searching
  - The World Wide Web
- I also provide some details about current audit resources which are available via Listservers, Usenet news groups and the World Wide Web.

What is the Internet?

It is not a single network, rather it is a network of networks which grows and shrinks every day as new resources are added and others disappear.

There are some impressive statistics.

- Two million computers connected with 15 million users.
- Over 4 trillion characters of information available on-line.
- 4 million home computers connected.
- Ten thousand new users every month.
- 6 out of ten subscribers use the net for their work!

Each of these computers and each of these users has the potential to connect with all the others and share information; across national, cultural and religious divides.

These statistics are actually out of date now. The true numbers are probably considerably higher.

Given that these statistics are probably a year out of date, what is the prospect for the future? The Bangemann report to the EC in 1994 tried to promote the use of communications technology for the benefit of the EC. With growth like this, what hope do governments have of controlling the resource!!! Whether they adopt it or not, it's going to happen.

One point to remember is that the Information Superhighway promoted by both the Bangemann report and by Al Gore is **NOT** the Internet as it exists today. The Internet is somewhat of an Information Cart Track. It has ruts to trip us up and large muddy puddles to swamp us. It also has Information Highwaymen lurking around the corners trying to rob us of our information and subvert our communications. The real Information Superhighway is some years off. Although elements are being constructed, it has still to be built. Until it exists and is safe, we should be "learning to drive" on the Cart Track that exists today.

Going On-Line

How do we get on line and use the resources?

First, we need the equipment. A modem, some software and a suitable connection. The modem is the easy bit. Buy one anywhere; but, be sure to get the fastest one

you can. Facilities like the Web are pushing so many bits down the line that you need to be able to talk to the net as fast as you can.

Software is not a problem. Most service providers will provide suitably tailored software with the connection.

Therefore, the main question is "Who to buy a service from?"

There are basically three levels of connectivity.

Firstly, there are networks like CompuServe which are closed and provide their own services. They are now also providing gateways into the Internet. Costs are normally based on a monthly fee, plus a charge for connect time and for connection to particular services. Plus of course the cost of the telephone call to connect.

Secondly, remote access via a service provider. This is potentially the most common route for the future. The service provider has a direct connection to the net and subscribers dial in remotely to them to get connection. This is the access method which I use personally and is potentially the cheapest method. Most service providers will charge a monthly flat fee plus of course the telephone costs.

Finally, the most expensive option of all. A direct connection to the Internet is the sort of option which is chosen by academic institutions and some major companies. It is expensive because you need to maintain computer equipment with the associated staff costs and, are generally connected directly to the Internet 24 hours a day, 7 days a week via expensive high speed leased lines. This is not recommended for normal, casual use.

So, now you are connected to the Internet, what are the facilities that we can use?

Electronic Mail

Firstly, and most importantly is electronic mail, commonly referred to as e-mail. E-mail makes up the bulk of the traffic on the Net. It is the workhorse of communication and is certainly the facility from which I personally gain most benefit.

In fact, most of what I describe in this paper can be accessed using e-mail.

I took to using e-mail initially as my main vehicle for using the Net as it was often said that "you don't get viruses from e-mail". Even I have used that as an excuse. **DON'T BELIEVE IT....YOU CAN.** I will mention this one again later.

One thing to be aware of with e-mail is that, unlike the traditional Post Office, if you make a slight mistake in the address, the mail cannot be delivered. The addresses are very precise and must be transcribed exactly or there will be no delivery. To be fair however, unlike the Post Office, if the mail cannot be delivered it is returned with a note to that effect, so at least you have the opportunity to send it again.

However, network links can go down at any time and mail can be delayed or disappear into a "black hole" never to be seen again.

There are strict formatting rules which, when you understand them, make remembering and interpreting addresses easy. Firstly, the e-mail addresses are actually an extension of what is termed the IP address. These Internet Protocol addresses are actually a combination of the user name and the address of the computer that they use to access the Internet. IP address allocation is controlled and the addresses must be registered. If you connect via a service provider, that is all you need to know. You will be allocated an IP address by your service provider and a user name, although you can sometimes choose your own user name.

IP addresses are numbers. It was accepted that numbers are difficult to remember, so these are translated into names. Once again the names are unique like IP addresses. When you connect to the Net, the names are translated into numbers which are then used to determine the route to the required destination.

The addresses are always in the format of:

Username@subdomain.domain

The subdomain can be a single or several elements. The domain is always a single element in the address. For example, my own IP address is:

alan.oliphant@dial.pipex.com

where:

alan.oliphant is my user name

dial.pipex is the subdomain

com is the domain

Once you understand the concepts of addressing and using e-mail, it's time to get some more value from the net.

Listservers

Listservers are mailing lists which some interested party maintains on their computer for a particular topic. The listserver is actually the software programme which maintains the list.

Sending a note to the listserver with a SUBSCRIBE command in the body of the e-mail message automatically puts you on the mailing list. You will then start to receive all the mail handled by that listserver for the particular list you have subscribed to. A listserver can handle many mailing lists, each one of which has a unique name.

They are conferencing systems. You can contribute to the discussions or ask new questions of the recipients by sending an e-mail message to the particular list (not the

listserver). This mail is then automatically redirected to all the people who are subscribed to the list.

This is actually one of the main uses that I get from the net. If I have a particular question, I mail it to the appropriate list and wait to see if anyone wishes to help or offer advice. I tend not to have to wait long.

One problem here is that the unscrupulous can just take an existing subscription list and add it to another to use to send junk e-mail. This has happened once to me (and the rest of the subscribers). However the good thing is that the listserver software also allows you to unsubscribe by sending the relevant commands to the listserver software. Junk mail is an irritant, but one that you can solve yourself.

Usenet Newsgroups

USENET is a similar mechanism, but applied differently. Usenet messages are carried across the whole Net, rather than just emanating from one site like the Listservers. Usenet messages travel across the whole Net and are normally stored by your host computer (i.e. service provider). Thus the messages are duplicated across many hundreds (if not thousands) of sites across the world. The Usenet messages are organised into Newsgroups where each group covers a specialised topic. At my last count, my own service provider carried in excess of 9000 of these groups.

The concept of communication is the same as for Listservers. Send an e-mail message to the group and it will be proliferated across USENET to all the news servers around the world. If anyone replies to the message it will again be posted to all servers around the world and you can read the answer and post additional questions and so on. With this sort of global coverage there has to be some sort of order imposed otherwise chaos reigns. The Newsgroup names are organised into a strict hierarchical order with the first part of the name determining the type of group.

Getting a new group set up means getting the full name registered and that is not a simple matter.

There is a specific group for internal audit matters. This is the alt.business.internal- audit group. The fact that it is in the alt hierarchy (controversial or unusual topics) is something I will leave you to speculate on yourselves. Let us just say that I helped set up the group and it was not easy. This was a compromise which is still being debated.

FTP

FTP stands for file transfer protocol.

Simply stated, log on to a remote machine, search through its directory structure, find the files you want and download them to your machine.

The greatest source of viruses ever! Especially when the site you log on to has no control over who is allowed to upload files to their machine to be available for others to download. Be warned! If you do not know the site you download from, virus check everything or don't do it. This is made worse by the concept of anonymous logon. Given the potential 15 million users across the net who can potentially log on to and FTP site, it would be impossible to have an individual logon for each. Hence they allow you to log on with the name "anonymous" and give the password of your full e-mail address. Then you may be allowed either limited or full access to the hard disk of the machine you have connected to. I have yet to come across a case where full access is allowed, but I have heard that there are cases.

If all you have access to is e-mail, don't despair. You can send an e-mail to an FTPmail site which contains commands that tell the server which files you wish to download and where they are located. The FTPmail server will retrieve the files and send them to you via e-mail. Hence my earlier warning. If you wish to eliminate the risk of viruses by prohibiting FTP server and client software from your site, the controls can still be bypassed using e-mail. BEWARE.

All this is very good, provided you know what you are looking for. In many cases, you know information is out there, but if you don't know the name of a file or the site that holds it, you can't hope to find it. This is where facilities such as Archie come in.

ARCHIE

Archie is a search programme.

Archie is actually a collection of servers. Each of these servers is responsible for keeping track of file locations in several different anonymous FTP sites. All of the Archie servers talk to each other, and they pool their information into a huge, global database that is periodically updated. You can search this database for file locations simply by giving an Archie client or server a keyword to search for. Archie doesn't retrieve the file, but it does tell you exactly where the file that you are looking for is located. Once you know the file's location (and its filename), retrieving the file using FTP is easy.

Once again, if you don't have the necessary software to use, you can carry out a search by sending an e-mail letter directly to an Archie server. The server will eventually send back an e-mail containing details of the results of the search. Then a simple e-mail to an FTPmail server and the files are downloaded.

GOPHER

Gopher takes the concepts of Archie even further. It is a menu-driven application that allows you to hop around the globe looking for information. Gopher's interconnected menus allow you to "burrow" deeper and deeper until you find the information that you are looking for.

Why is Gopher so special? Well, unlike Archie which

just tells you where the information that you want can be found, Gopher actually goes out, GETS the information that you want, and puts it on your computer screen! Once again there is Gophermail software which allows you to use e-mail to generate the searches and retrieve information.

While this use of e-mail to carry out searches and retrieve information may be seen as a way of bypassing controls, it can actually be very useful for those people with the level 1 connection (via a gateway) where the only Internet facilities they are allowed is e-mail. They can get increased connectivity for little extra cost

World Wide Web

The World Wide Web is the fastest growing facility on the Internet. Why? Because it is based on hypertext and supports multimedia; it makes for good television and is very sexy. Unfortunately, it is also very resource hungry and gobbles up great chunks of bandwidth on the net. The more it is used, the more data flows and the Net tends to slow down. Unless more, faster, higher capacity lines are installed I suspect that the Web could actually cause the Internet to drown and die. Perhaps I am being melodramatic.

It exploits the concepts of hypertext. Very briefly (and simply) hypertext consists of documents (referred to as pages) which can contain embedded objects (such as graphics, video and sound) and embedded links to other pages or even other Web servers. Thus, when reading a hypertext document, you can select a highlighted area and watch related videos, listen to sounds, or be linked to another related page on the same server or even one on the other side of the world. This is a, somewhat, simple description of a complex technology.

If you have Web software installed it will allow you to access Web pages properly, carry out Gopher searches, download using FTP and send e-mail. It also has its own sophisticated search engines. In fact, if you don't have the software, you can also access it via..... you guessed it; there are Web mail sites now to allow you to access the Web sites via e-mail. Somewhat slower than using the specialised software, but it still works.

There are more and more sites which are being developed specifically for internal auditors.

Netiquette

This would seem to be an appropriate point to raise the issue of Netiquette. E-mail is a wonderful medium for communication. It is cheap, available world-wide, almost instantaneous and can carry succinct messages. However, it lacks the benefits of verbal face to face communication. It cannot carry the subtle nuances of tone or body language. What may seem like an innocent comment can be taken for a rude remark. Beware!

Also, we all need to remember that we are communicating across national boundaries with peoples of different cultures. Tolerance is the watchword. Other cultures do not share our opinions or tolerances and vice versa. Do not get incensed by others' attitudes or get involved in hurling insults across the Net. It helps no one. The best advice is to "lurk"! Read the messages and gauge the tone of the more experienced contributors. Then dip in a toe and make a few contributions. If you get too aggressive or violate the accepted norms of accepted behaviour, you may get either a gentle reminder (as I did with my first indiscretion), receive abusive mail in return (as happened on a recent occasion when one of my humorous comments was taken seriously) or get flamed (flooded with thousands of messages to crash your computer) which has not yet happened to me but is not unknown.

The Downside

The Internet is by its very structure (or lack of it) inherently insecure. Even if you are aware that a computer with which you are communicating is secure, you have no way of knowing whether the machines or communications lines through which your messages are routed are similarly secured. In fact, the ease with which new machines and additional networks can connect to the Internet means that it is in a constant state of change. The simple message is "TRUST NOTHING".

The dangers are fairly obvious and it is not the intention of this document to dwell too much on the technical security issues. However, the following risks need to be borne in mind.

Viruses

As you can have little trust in the security over sites to which you connect, you cannot be certain that files which you download via FTP are not infected by viruses. The simple rule is to virus check everything as soon as it is downloaded. As most files downloaded in this way are compressed in one way or another to reduce file sizes, they need to be decompressed before scanning. One other feature of compression software is that compressed software can exist as self-uncompressing executable modules. The executable module will decompress itself when run. The compressed executable could be infected, or the underlying compressed executables could also be infected. Thus you will need to virus check both before and after decompressing.

To make matters worse, commercial virus checkers are behind the times. They tend to have their virus signature files update on a regular basis, but only as a result of a new virus being detected. These newer viruses tend to be transmitted via the Internet, so you will probably catch a new virus from a downloaded file before you have had you virus checker updated and will therefore not detect it. Therefore, don't rely solely on virus scanners to detect all known viruses; they can't. Preferably also have memory resident virus detectors looking for unusual system calls and use those which create and check file lengths etc.

It is also advisable to use a stand-alone machine for connection to the Internet if you are contemplating file downloading. If you get infected, the damage is minimised. You may have thought that it is only executable modules (i.e. programs) which can transmit viruses and infect machines. Don't believe it. The rise of the World Wide Web has introduced a new risk. If you use a Web Browser it can be configured to open an application to view a particular file type. If you configure your browser to open Microsoft Word for Windows in response to a .doc type file, it is possible to imbed macros within the document that are very powerful and harmful - and which are triggered by particular key strokes. The WFW macro language is now a dialect of Visual Basic - a very powerful programming language. You must be ever vigilant and take nothing on trust.

Hackers and Crackers

Then there are the hackers (or strictly speaking, the crackers). If we have level 3 access to the Internet (direct access) there is the potential for the hacker to connect directly to you and wreak havoc. This is not as great a problem if you only have level 1 or 2 access although the hacker can still connect to your service provider and use your account for whatever purpose.

The main defence against people who want to break into your account is your password. Keep your password secure, and you should never have anything to worry about. Give your password to others, or write your password down and put it near your computer, and you are asking for trouble. Don't make it easy for the hacker. There are some KEY points you need to remember to protect yourself and your account:

* NEVER give your password to anyone.

* NEVER write your password down, and especially never write your password anywhere near your computer.

* NEVER let anyone look over your shoulder while you enter your password.

* NEVER e-mail your password to anyone.

* DO change your password on a regular basis. A good rule of thumb is to change it at least every month.

* DON'T pick a password that is found in the dictionary. When you set your password, it is encrypted and stored into a file. It is really easy for a hacker to find your password by encrypting every word in the dictionary, and then looking for a match between the words in his encrypted dictionary and your encrypted password. If he finds a match, he has your password and can start using your account at will.

* DON'T use passwords that are foreign words. The hacker can also get a foreign dictionary.

* NEVER use your userid as your password. This is the easiest password to crack.

* DON'T choose a password that relates to you personally or that can easily be tied to you.

* DO use a password that is at least eight characters long and that has a mix of letters and numbers. The minimum length of a password should be four to six characters long.

* NEVER use the same password on other systems or accounts.

* ALWAYS be especially careful when you telnet or rlogin to access another computer over the Net. When you telnet or rlogin, your system sends your password in plain text over the Net. Some crackers have planted programs on Internet gateways for the purpose of finding and stealing these passwords. If you have to telnet frequently, change your password just as frequently. If you only telnet occasionally, say, for business trips, set up a new password (or even a new account) just for the trip. When you return, change that password (or close out that account).

The best passwords (the ones that are the easiest to remember, and the ones that are the hardest for hackers to crack) are those that are effectively mnemonics. Think of a relevant sentence and use the first letters of each word as the password. Sentences are EASY to remember, and they make passwords that are nearly impossible to break. If you notice odd things happening with your account:

1. Change your password IMMEDIATELY!

2. Tell your local Internet service provider about it.

It is very common for someone whose account has been hacked to dismiss the signs as technical problems with the system. However, when one account is hacked, it very often puts the whole system at risk.

There are other more complex methods of hacking that are more difficult to foil. IP address spoofing is becoming a greater threat. This is where the attacker assumes your IP address to fool security controls and gain access to your space. I will not describe in detail how it is done as it would take far too long and others have written much on the subject. Just bear in mind that it is a growing threat with some 170 reported incidents in June 1995. I do not know how many attacks went undetected.

Confidentiality

Remember that all traffic across the Internet is in plain ASCII. It can be read and you don't know by whom. Do not give away company secrets when communicating via e-mail. While the use of encryption provides the best protection. However, as there are restrictions on the use of encryption technology this cannot always be an easy option. It has often been said that, "If you would write it on a Postcard, you can trust it to the Net".

Firewalls

A firewall is effectively another computer which sits between your main computers and the Internet connection. This filters the traffic and can be used to impose restrictions on the facilities which users are allowed to connect to. Firewalls can get very complex and it is outside the scope of this document to explain their use in more detail. The simple advice is to get your technical support staff to advise.

Costs

Then there are the costs. My own service costs a monthly rental plus telephone charges. I connect as little as possible as I am paying the call myself. If you set up a connection from work, consider the costs first. This should include the cost of the service, the connection charges and, more importantly, the staff costs involved. The cost in terms of staff time will probably be your greatest expense as "surfing the Net" can become an addictive habit. In any event, if an auditor is spending his entire day playing with the Internet, it is actually a management issue, not a technical one. Auditors are paid to audit, not to surf the Net!

Garbage

Beware of the garbage! The Internet is full of it. Merely because information resides on a computer doesn't mean that it has any value. The Internet is open to all and attracts all sorts of people with some fairly extreme views. Be prepared to sift out the dross to find the pearls.

Conclusions

The Internet has reached adolescence in North America. In the UK we have barely got into Primary School. Over the next five years, the Internet or the Information Superhighway or whatever you wish to call it will reach maturity. I would like to think that the Internal Audit Community in the UK can move out of their short trousers very quickly and lead the world in this area, rather than just following it.

What are the benefits to me? Briefly, over the last year I have been able to keep in regular contact with like minded internal auditors across world. Some of them existing colleagues and others new friends; all of them dedicated professionals who, even though all are not members of the Institute of Internal Auditors, appear to live by its motto of "Progress Through Sharing". In fact, I was able to re-establish contact with two ex-colleagues whom I had not spoken to for more years than I care to remember, one in Singapore and one in Hong Kong. Then we had a case some months ago where we were asked to carry out a review in Spain where we had no knowledge of the technology being used. Trying to get staff geared up to carry out this type of audit in a limited time (we had a week to carry out the review and a month's notice) is not easy. Trying to identify a suitable training course is difficult enough, finding one in the timeframe necessary is impossible. However, one message posted on a suitable internal auditing list produced advice and a complete audit programme within 48 hours. The result was a job well done.

I have been able to access FTP servers containing audit programmes, sample security policies and standards, reports on auditing issues. I even use the Net as a research tool for the final MBA project I am carrying out. For this, I have collected enough material to enable me to do a PhD!

If I were to try to get a similar level of feedback using existing contacts via telephone and letters, I suspect I would still be trying. Nothing against my colleagues who have yet to get tapped into the Internet; they are restricted by pressures of work as am I. However, with e-mail, the lists and newsgroups, all you have to do is post a question and any one of the (potentially) thousands of readers can get back to you with a response.

Finally, a warning about the quality of responses. While the responses which I receive at the moment are of good quality, this is no cause for complacency! I attribute the current quality to the professionalism of the active contributors. They are the pioneers, exploiting the technology for the benefit of the profession. However, after the pioneers come the settlers, the gamblers, the exploiters of the resources (sorry for the Wild West analogies). I suspect that the quality may fall over the coming years. Learn to be selective in the advice you are given. Also, if you connect and take advice from all the dedicated professional, be prepared to give something back. Everyone has something to contribute, however small it may seem. It may seem small to you, but to another beginner, it may be manna from heaven.

Audit Specific Resources

Now for a bit more detail about specific resources that have been set up with the internal auditor in mind. For any internal auditor intent on going on-line, Jim Kaplan maintains a list of current resources. This list is a the definitive first stop for all new audit users. It is updated constantly as new resources are identified and is posted regularly on various listservers, the alt.business.internal-audit Newsgroup and some web sites. It is best viewed at Jim's web site on:

http://www.unf.edu/students/jmayer/arl.html

It is the starting point for new users as well as a point of reference for the more experienced. The following list of interesting resources was actually taken from Jim's list with his kind permission. Jim Kaplan is to be applauded as one of the true pioneers of the internal audit profession.

In the examples which follow, Web sites are characterised by addresses which start: - http://www..... This address is referred to as the URL (Uniform Resource Locator). AuditNet Accounting, Audit, and Financial Management E-Mail Directory (AAF) - This is a collec-

tion of personal e-mail addresses, mailing list information, and any other means of related information that includes the use of e-mail.

The URL is
http://www.unf.edu/students/jmayer/email/home.html

ACL Software Users Discussion List - ACL-L is a non-moderated Internet discussion list and forum to exchange ideas and information among authorized users of ACL (Audit Command Language) software which is relied on by more than 10,000 users worldwide. Send subscription request to listserv@etsuadmn.etsu.edu with one line in the body of the letter: SUB ACL-L yourname.

ANet Mailing Lists - Anet is a networked electronic forum in the broad accounting and auditing discipline as follows.

AAUDIT-L (Audit Issues)
ANews-L (Accounting/Auditing News)
AAccSys-L (Accounting Systems)
AEthics-L (Ethics in Accounting and Auditing)
AFinAcc-L (Financial Accounting)
AIntAcc-L (International Accounting)
AMgtAcc- L (Management Accounting)
ATeach-L (Accounting Education)

Subscribe to lists by sending e-mail to LISTPROC@scu.edu.au. In the body of the message type SUBSCRIBE followed by listname and your real name. ANet World Wide Web site - The site maintains archives of the 30 Anet mailing lists, complete list of accounting organisations world-wide, an accounting bibliographic database, and a variety of accounting and auditing resources.

The URL is http://anet.scu.edu.au/anet

Association for Computing Machinery (ACM) - largest and oldest international scientific and educational computer society in the industry. ACM provides members with a forum for sharing knowledge on developments and achievements. There is a Special Interest Group (SIG) for Security, Audit and Control.

The URL is HTTP:\\acm.org:80

Audit-L Discussion List - A generalised audit discussion list open to all auditors irrespective of industries and organisations. The list is intended to have a diverse membership so that broad perspectives from all auditors could be gained through interactive communication. Send subscription request to listserv@etsuadmn.etsu.edu with one line in the body of the letter: SUB AUDIT-L yourname.

Auditor General of Canada - The 1994 Annual Report of the Auditor General of Canada is now available on the Internet. Reach the report by gopher access as follows: gopher.phoenix.ca.

The URL is gopher://gopher.phoenix.ca:70/

Barefoot Auditor(BFA) - Pathfinder, the company that produced Barefoot Auditor, a software auditing program established a WWW site with FTP facilities for program demos and sharing information about how to use BFA. Includes press releases, an introduction to software auditing technology, and information about other network security review tools.

The URL is http://www.u-net.com/pathfinder

Computer Operations, Audit, and Security Technology (COAST) Project - computer security research project in the Computer Science Department at Purdue University. Exploring new approaches to computer security and computer system management. COAST has a comprehensive FTP archive containing nearly 400 Mb of tools, papers, technical reports, documentation, announcements, alerts, security patches, and newsletters.

The URL http://www.cs.purdue.edu/coast/coast.html

Computer Security Resource Clearinghouse (CSRC) - The NIST Computer Security Division maintains an electronic clearinghouse to encourage the sharing of information on computer security. The CSRC contains computer security awareness and training information, publications, conferences, software tools, as well as, security alerts and prevention measures.

The URL is http://csrc.ncsl.nist.gov/

Computer Security Publications from NIST - send email to docserver@csrc.ncsl.nist.gov with the message "send index" for a list of NIST computer security publications. To retrieve copies of the publication via e-mail, send message "send <document filename>". The NIST also distributes a Computer System Security Laboratory Newsletter via the Internet. Send e-mail message to mailserve@nist.gov with the message "subscribe csl-newsletter".

Columbia University Internal Audit - The Columbia University Web site has a section devoted to their Internal Audit Department. The section includes A Guide to Internal Controls, Internal Control Issues, and Auditing at Columbia University: A Service to Management. The last document is an excellent guide that other audit organisations could follow to educate management and departments about internal auditing.

The URL is http://www.columbia.edu/cu/ia/

Cryptography, PGP, and Your Privacy Web Page - contains links to many of the Web's resources on cryptography, as well as lots of documentation on the Pretty Good Privacy (PGP) encryption program for PCs, Macs, and Unix.

The URL is
http://draco.centerline.com:8080/~franl/crypto.html

CTI-CCC-AUDIT - Auditing and accounting mailing list sponsored by the CTI Centre for Accounting, Finance and Management at the School of Information Systems, University of East Anglia, UK. The list is open to anyone interested in Auditing and wanting to be in contact with others with similar interests.

To subscribe send an e-mail message to mailbase@mailbase.ac.uk and state in the message:

Join cti-acc-audit Firstname Lastname.

Firewalls FAQ's - As organisations establish Internet connections, auditors are asked to review security issues associated with connectivity. Frequently Asked Questions or FAQ's may help auditors address some of the issues.

The URL is
http://www.tis.com/Home/Firewalls/FAQ.html

General Accounting Office - GAO is constructing a WWW homepage. The site currently includes decisions of the Comptroller General of the U.S.

The URL is http:/www.gao.gov/decisions.html

General Accounting Office Reports - GAO high risk, miscellaneous, technical, and transition reports available.

URL is http:/./www.yahoo.com/Government/
Agencies/General_Accounting_Office/

Government Auditing Standards - The GAO Government Auditing Standards or Yellow Book is available at:

gopher://pula.financenet.gov/00/docs/central/gao/yellow

IAWWW - The Internal Auditing World Wide Web ia available, on a temporary and non-production basis, at

URL: http://WW01.DHMC.DARTMOUTH.EDU/

The Institute of Internal Auditors (United Kingdom) - The IIA UK have set up a World Wide Web site to provide a service to members (and others). This site is currently being constructed and can be found at the temporary location of:

URL is http://www.easynet.co.uk/iia/

By the time this article is published, it should have found a more permanent address. This can be found by reference to Jim Kaplan's list.

The Central Indiana Chapter ISACA created a list for information systems auditors called CISACA-L. The list is meant to encourage professional discussion and is open to all information system auditors. To subscribe send a one line message to listserv@vm.cc.purdue.edu with the message SUBSCRIBE CISACA-L (yourname). Messages sent to CISACA-L@vm.cc.purdue.edu will be distributed to all subscribers.

The New England Chapter ISACA created a list for information system auditors The list is open and seeks to encourage professional discussions. To subscribe send an e-mail message to listserv@mitvma.mit.edu and provide the following: SUBSCRIBE ISACA-L yourfirstname yourlastname

New Mexico Chapter of the Information Systems Audit and Control Associations now has a home page on the World Wide Web. Includes information about meetings, professional development, conferences and the CISA program.

URL is http://www.cabq.gov/aud/isaca.html

Institute of Chartered Accountants of England and Wales Accounting Information Service, The ICAEW Summa Project is the site of the World Wide Web information server for accounting academics, students and professionals. The project is funded by a grant from research committee of the ICAEW. The WWW site is at the University of Exeter, Devon, UK. Provides access to a number of accounting, auditing, and finance related resources such as FINWeb, EDGAR, the Security and Exchange Commission's online database, the Financial Executive Journal, Global Network Navigator (source of information about Internet resources), and more.

The URL is
http://www.ex.ac.uk/~BJSpaul/ICAEW/ICAEW.html

Internal Audit Newsgroup - (Alt.business.internal-audit) Internal audit newsgroup formed September 5, 1994 for discussion of internal auditing related subjects. Open forum to share ideas, proposals, experiences, hopes, fears, and vulnerabilities. Access via Usenet newsreader.

International Organisation for Standardisation (ISO) On-line - ISO, the organisation that developed standards for quality management, established an on-line support unit to provide facts on ISO 9000. The ISO 9000 Forum provides answers to various frequently asked questions as well as background information on the standard.

URL is http://www.iso.ch/9000e/forum.html

RISKWeb - Information resource for academics and professionals interested in risk management and insurance issues. The RISKNet WWW server is a service of the RISKNet mailing maintained at the University of Texas at Austin. The RISKNet mailing list provides individuals around the world with a forum for open discussion of Risk and Insurance issues.

The URL is
http://riskweb.bus.utexas.edu/riskweb.html

Software Publishers Association - The Software Publishers Association (SPA) sponsors a forum on CompuServe to keep members of SPA, developers and users of computer software aware of SPA activities and developments. Members of the SPA are available on-line to answer questions about publishing software such as how to obtain a copyright for a newly developed program and to audit multiple computers for pirated programs.

The URL is http://www.spa.org

These are examples only. The full list is considerably more comprehensive and grows all the time. Internal auditors who discover new resources are urged to submit details to Jim who will include them for others to use.

Alan Oliphant is The Computer Audit Manager with The Standard Life Assurance Company. This paper is based on an article which was originally published by Elsevier Sciences in Issue 4 of Computer Audit Journal and which was presented at COMPSEC 95.

Message from George Allan

Hi everyone,

I am George Allan the new Academic Editor of our CASG Journal. I sort of volunteered after the Chairperson John Mitchell approached me with incitements, incitement and threats such as:-

"We really need you"
No you don't, you need an editor.

"It will look good on your CV"
I'm not applying for a job.

"It will be good experience"
I have all the work I can handle.

"Oh all right! We can't get anyone else!"
I'll do it

So, here goes.

The purpose of any journal is to report on achievement and the latest research to as wide an involved audience as possible. There are fundamentally two kinds of article published in learnèd journals.

One is the *academic type* article reporting on research, development, new methods, advanced techniques, and new thoughts & ideas.

Then there is the *reporter type* article which may tell of a real-life experience relevant to the readership.

A journal is only as good as its articles and its readers' involvement. I would encourage many of you to take up the pen and write down your thought and ideas. Try turning then into an article for submission. Academic articles will be refereed by an active panel of specialists. This adds to their worth in the academic world and does look good on CVs. Applications to join the referee panel should be addressed to me at the University of Portsmouth please.

I do ask all would-be authors to follow the Harvard system of bibliographic references please. What is a reference you may ask? Well, in your article you may wish to quote another piece of work by someone else. In the text you refer to the published work by mentioning the author's name and year of publication in brackets such as ALLAN G.W.(1994). At the end of your article I ask you to list all these references in alphabetical order of author's surname. This is known as ***the bibliography*** and readers refer to this when they come across ***a reference*** in your article.

A reference is a set of data describing another publication, or part of a publication, and sufficiently precise to enable anyone wishing to read that other article to identify it without searching for further details. This enables them to follow it up as a result of reading *your article*. It also gives your article credibility and substance. So, how do you do it? It is fairly straight forward providing that you follow a few basic and simple guides and get used to putting information in a particular order.

The bibliography lists all the articles that you have made reference to in the following way. 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. "This is the Title of the Article" Next you print the title of the book/journal/periodical/magazine in which the article was published. This is printed 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) which tells people which part of which volume to look in....I'm told that it's OK to end a sentence with a preposition now-adays!!

So there we are - the simplified Harvard system which will probably be adequate for our needs at present. Do think about writing something, even if it is only a draft to see what the reception is going to be like. But be warned...although successful writing is immensely satisfying and a heady aphrodisiac for mental stimulation and greater goals, it is also quite hard work and takes a long time. The most difficult part of writing any article is to get the pen to actually touch the paper for the very first time.

Good Luck

George Allan

Longevity of computer records:
some implications for computer audit.

Dr. Andrew Hawker

Abstract

The archiving of data using optical and magnetic storage media depends on careful planning to ensure that the data will actually be readable, and where necessary, capable of being authenticated, at some point in the distant future.

Computer auditors should be actively involved in planning and implementing archive systems, and in doing so should consider whether their organisations have two specific mechanisms in place - for "time transfer" and "trusted conversion".

Keywords: Archive, Authentication, Computer Audit, Longevity, Record Retention.

Introduction

Paper records have demonstrated their ability to survive over hundreds of years.

Magnetic storage media, in contrast, have been used in commercial computing for just over thirty years, and optical storage media for almost half that time.

Paperless working in factories and offices implies that more and more evidence will, in future, have to be retrieved from paperless archives.

Auditors need to be mindful of the demands for information which could arise some years ahead, and to help in developing retention policies which will ensure that it will be possible to locate and read the data and, where necessary, authenticate it.

Public archivists, who are concerned with preserving a very wide range of materials, not just business records, have already expressed disquiet about the implications of depending on records originating from computers (see for example Mohlhenrich, 1993). Since their role is to preserve material for future generations, they take what could be regarded as an ultimate long-term view.

Other commercial and government organisations also need to be able to ensure access to records over many years. This may be a direct consequence of the business they are engaged in, as in the case of insurers or pensions providers. Or it may be that they have entered into contracts to provide long-term services or warranties for their products. Almost all of them will need to consider the possibility of disputes over taxation, where the normal limitation is six years but where, if there are suspicions of negligence or fraud, investigations can go back twenty years (Taxes Management Act 1970, section 36).

Three basic questions which relate to the longevity of computer-generated records have been expressed succinctly by Helms:

"Will the medium survive? Will there be equipment that can read the medium? Will the data stream on the medium be understood?" (Helms,1990)

A more detailed list of possible concerns has been provided by Carty, who suggests that consequences of a move to electronic archiving can include:

- records are less likely to be created by staff who are trained in filing conventions
- the long term "shelf-life" of records may be difficult to assess
- IT equipment and software can become obsolete very quickly
- electronically stored records can attract the attention of those with malicious intent
- it is relatively easy to destroy large numbers of records accidentally
- it is relatively easy to remove large numbers of records deliberately (Carty,1994).

All of these concerns are within the province of the computer auditor. However the costs of addressing all the concerns and setting up archives which are completely "future-proof" can be enormous. Besides ensuring that record retention is taken seriously, the computer auditor must assess whether storage policies make sense in terms of their effectiveness and economics.

Storage Technology

In 1962, the LEO III computer was modified to enable it to exchange data via magnetic tape with an ICT Pegasus 2 machine (Bird,1994). This was one of the first examples of the use of magnetic tape as a general purpose medium for data storage and transfer, a role which was given much greater impetus when IBM introduced its 2400 series of tape drives for the 360 processors in 1965 (DeLamarter,1988). In the mid-1980's the US National Bureau of Standards published reports on the longevity of ferric oxide tapes, by then widely used throughout the computer industry, and suggested that providing tapes were stored carefully they should last for twenty years (Saffady,1993). However, new tape

technologies, incorporating cobalt and chromium, were emerging at about this time, and early versions of optical data disks were also beginning to make their way onto the market. Purchasers were confronted by a bewildering choice of products, each offering its own particular combination of density, speed and ease of use. Product lifetime was rarely a factor in the purchase decision, a situation which, to judge by the features highlighted by vendors, still prevails today. Perhaps because of this lack of consistent assurances from the suppliers, a convention appears to have grown up of re-copying tapes on a regular basis every ten years or so (Eaton,1993).

The longevity of each medium depends on a number of factors, and the difficulties of making accurate predictions have been explored by Arps in respect of CD-ROMS (Arps,1993a). With each new advance in materials or production methods, the best that a manufacturer can do is to subject the product to stress tests over a relatively short period time and then extrapolate from these to forecast how long the medium will survive in real life. Such estimates cannot be all that precise. They must be based on assumptions about the levels of error which can be accepted and the range of conditions under which the medium will be stored. Variations will also occur between different disks, either because of variations in quality achieved during manufacture, (Arps, 1993b) or because different times are allowed to elapse between the manufacture and the actual process of writing onto the disk (Avedon,1994).

Archiving therefore has to involve the setting of appropriate specifications for both the medium *and* the environment in which it is going to be stored. Some designs for storage systems depend on a centralised method of control, particularly where security is important or where a variety of different types of object are to be managed: (see for example Schlatter, 1994). However, many organisations hold their data in a much more dispersed or fragmented way. In some instances, storage may be undertaken by outside contractors. In such situations it is difficult to lay down and enforce standards governing the way the data is held, and if for any reason the storage medium ultimately proves to be unreadable it is likely to be extremely difficult to pinpoint where the blame lies. This would seem to be a responsibility which an organisation should strive to keep under its own direct control, and thereby more easily within the remit of its own internal audit team.

The second question raised by Helms, on whether or not equipment will exist to read the medium at the appropriate time in the future, is an intriguing one. Most of us would find it frustrating, no doubt, to discover that some vital data was could only be obtained from a 5.25 inch floppy (or even a 3.5 inch diskette as formatted by an early Amstrad). Equipment to read such media still exists, although it can be time-consuming to track down. It is feasible, though expensive, to build bespoke disk drives. Where this problem may return to haunt us, however, is when the costs involved in finding or building appropriate equipment start to arise at some unspecifiable point in the future.

If obsolescence is perceived as a serious risk, then the best solution is to pre-empt it by making copies onto a brand new type of storage medium at regular intervals. The crucial question then becomes: which will last longer - the medium or the means of reading it? Experience to date suggests that in many cases it is the former. Seen in this light, the longevity of the medium itself ceases to be the crucial factor which it might otherwise seem to be.

The relationship between data and software

Reading information from the past can be compared to reading information from a telecommunications network. The physical layer, represented by a disk or tape drive, may be able to deliver you an error-free stream of bits, but this is no guarantee that you will be able to make any sense of the data. To do this, some knowledge is required of the software which generated the bit stream in the first place (Rothenberg, 1995). If the data comprises a string of ASCII characters or a raster-scanned image then decoding may be quite straightforward. On the other hand, if it contains the transaction log created by an in-house accounting system with a large number of users, it will be interpretable only if complete information is available about the version of the software involved, along with a wealth of salient information on the configuration of the system, the identities of its users, and so on. Somewhere in between these two extremes lie all the "standard" formats used for data interchange. These, unfortunately, tend to suffer from changes in fashion - as for example with the once-popular Ashton Tate dBase formats, or some of the standards promoted with limited success by IBM, such as Document Content Architecture.

Furthermore anyone who, as an auditor, is interested using the record in order to authenticate the information in it will face some curious paradoxes. For the record to be truly authentic, it should be exactly as laid down by the original software - perhaps burned into read-only memory. However, for it to be easily interpretable at some future date, it would be preferable to have a version which is not quite so cryptic. It might be helpful, for example, to include field names or datatype codes repeatedly, embedding them in the data to make its meaning more self-evident. Similarly, if records are being transferred from old to new media because of concerns about the obsolescence of technology, it may be tempting to take the opportunity at the same time to "update" the data in some way to a more modern format. Each of these processes of translation, however, adds an element of doubt to the record. Has the translation been accurate? Have all the records been processed consistently and completely? In addition, of course, questions arise about the impartiality of the process, which is open to abuse as a way of filtering out or modifying information which is seen as potentially incriminating.

Let us assume, therefore, that the data is left exactly as it was originally recorded. In this case there are two

options. One possibility is for a copy to be kept of all the relevant modules of the software which created the records. This immediately raises questions about the prospect of whether or not an appropriate platform to run the software will be available in the future. Processors are, after all, just as prone to obsolescence as disk drives, and manufacturers will not commit to support backwards compatibility indefinitely. Alternatively one can rely on the development, in the future, of new software products capable of undertaking sophisticated interpretation of files - successors, perhaps, to the kind of file search and retrieval products commonly used by auditors today. However such an approach is based on wishful thinking. As Michelson and Rothenberg have pointed out, to understand software and re-create aspects of its behaviour it is necessary to have a complete and rigorous specification to work from. Very few software products actually have such a specification. Indeed, in many instances a complete description of how the software behaves can only be obtained from executing the software itself (Michelson, 1992). And if we depend on running the software, but have no platform on which to run it, we arrive back at the same set of constraints inherent in the first of the two options.

Transfers of data through time

To return to the parallels with telecommunications networks: laying down archives of data can be regarded as a process of transmitting messages to the future. Although future recipients of the message may well be working for the same organisation in the same building, it will nevertheless be wise to begin by assuming that they will have little or no understanding of the systems in use when the message was first created.

If data is regarded as being transmitted via messages, then authenticity can be provided by one of the proven methods of applying message authentication codes which have been developed for networking. The requisite key will have to be stored separately and securely, together with details of the algorithm used. If the main concern is authenticity rather than secrecy, the data itself can be left in the clear, and will therefore be readable even if the authentication codes are lost. If it proves necessary to copy from one medium to another then, providing the copies are exact, authentication will still be possible.

If in addition the data itself is to be encrypted, then the risks are higher. As Cheswick and Bellovin observe with regard to back-up tapes:

"One can make a very good case for encrypting the entire tape during the dump process - if there is some key storage mechanism guaranteed to permit you to read the year-old backup tape when you realize that you are missing a critical file" (Cheswick, 1994).

The obvious candidate to be the holder of keys and algorithms (whether for encryption or authentication) is the computer auditor. Having ensured the long-term security of these, the auditor can then take a fairly sanguine view on the way data is being copied or moved around. So long as the data is subject to good housekeeping its future retrieval and authentication can be guaranteed. The alternative, of trying to impose comprehensive logical and physical controls over all the data archives themselves, is likely to be extremely difficult in many organisations.

Trusted conversions

If archive material is to be copied from one medium to another and it is proposed at the same time to modify it in some way then there is a further role for the computer auditor. The auditor will need to establish whether any of the following types of changes will occur:

1. **deletion of data**. This may actually be a legal requirement: for example, principle six of the Data Protection Act requires that in prescribed situations personal information "shall not be kept for longer than is necessary" (Data Protection Act 1984 Schedule 1).

2. **transformation of data**. This could be at a very low level - for example, to alter the method of compression of an image. However, if changes are proposed to standard abbreviations, account codes, precision of dates and times or other values embodied in the data then the long-term implications may not be immediately obvious.

3. **additions to the data**. Efforts to add helpful annotations or explanations to the data could lead to subsequent confusion as to what had been recorded originally and what had been added later.

If the auditor already has control over the data by virtue of holding the keys necessary to de-crypt and authenticate it, this will effectively ensure that he or she has to be involved in the conversion. However, if the conversion involves the processing of large quantities of data, perhaps with associated objectives of slimming down data volumes and improving the indexing or speed of access, then ensuring that the whole procedure is trustworthy will take every bit as much effort as a more conventional audit.

Conclusions

Computer systems are mainly installed for the advantages which they bring in terms of their ability to access data quickly and subject it to rapid processing and evaluation. The longer-term fate of the computer-encoded data does not always receive much attention. As dependence on computer data increases, computer auditors will need to insist on more carefully designed and explicit policies for record retention: (the areas which might be covered are outlined by Skupsky, 1993).

This implies taking an active interest in some aspects of systems design and operation which traditionally have not received a great deal of attention from computer auditors. While the need for reliable logs and trails has been recognised from the earliest days of computing, the controls required in respect of the long-term

retention of a wider range of records often exist only in embryonic form. Computer auditors will need to strengthen their links with those involved in database management, media storage and the archiving function to ensure that data will remain accessible in the future while still remaining secure against unauthorised changes and intrusion. In achieving these aims, it should be possible to adapt some of the security techniques already developed for the secure transmission of data contemporaneously over networks.

References:

Arps, M. (1993a) CD-ROM: *Archival Considerations,* in Mohlhenrich, 1993 pp 83-107.

Arps, M. (1993b) CD-ROM: *Archival Considerations,* in Mohlhenrich, 1993 at p.98.

Avedon, D. (1994) Electronic Imaging 101 Part II - Optical Disks and Backfile Conversions. *Records Management Quarterly,* July, 34-38.

Bird, P.J. (1994) *Leo: the first business computer.* Hasler, Wokingham, at p 128.

Carty, A. (1994) *Requirements under the Public Records Act when using Information Technology.* CCTA/HMSO, London, at p 13.

Cheswick, W.R. & Bellovin, S.M. (1994), *Firewalls and Internet Security.* Addison-Wesley, NY, at p 15.

DeLamarter, R.T. (1988) *Big Blue.* Pan, London, at p 79.

Eaton, F.L. (1993) in Mohlhenrich, 1993 at p 44, (referring to the policy of the US National Archives).

Helms, R.M. (1990) Introduction to image technology. *IBM Systems Journal, 29* (3), 313-332 at p 331.

Michelson, A. & Rothenberg , J. (1992) Scholarly Communication and Information Technology: Exploring the Impact of Changes in the Research Process on Archives. *American Archivist,* 55 Spring 236-303 at p 300.

Mohlhenrich, J. (ed), (1993) *Preservation of Electronic Formats and Electronic Formats for Preservation.* Society of American Archivists/Highsmith Press, Wisconsin.

Rothenberg, J. (1995) Ensuring the Longevity of Digital Documents. *Scientific American,* January, 24-29.

Saffady, W. (1993) *Electronic Document Imaging Systems.* Meckler, London, at p 118.

Schlatter, M. et al. (1994) The Business Object Management System. *IBM Systems Journal,* 33 (2) 239-263.

Skupsky, D. S. (1993) Establishing Retention Periods for Electronic Records. *Records Management Quarterly.* April, 40-49.

Dr Andrew Hawker lectures in information technology at the Department of Accounting and Finance at the University of Birmingham. Previously he worked in technical support for IBM and Amdahl. He is a member of a research team concerned with accounting and record-keeping issues in primary health care.

AS400 HELP REQUIRED

Some of you will remember our guide to auditing IBM's AS400 operating system which was authored by Malcolm Lyndsey. Indeed, this valuable guide is still available for the unbelievable price of £15.00 from our membership secretary, Jenny Broadbent.

Since its publication however, OS400 has moved on and Malcolm's work commitments make it difficult for him to find the time to update it. He has very generously however, offered the publication for updating to anyone who is willing to put in a little effort. So, are you willing to help with this task? If so, let me know and I will put together an editorial team. Ed.

CASG MATTERS

MEMBERSHIP UPDATE

This column is edited by Jenny Broadbent our Membership Secretary. If you have any queries, or points, about membership matters, then please contact her at the address provided in the Management Committee list elsewhere in the Journal.

Welcome to our new members:

Mr I McCulloch, Mr S Robertshaw, Mr G Brown and Mr T Powis, West Wiltshire District Council

Ms H A Jewitt, Morgan Grenfell

Mr T Hughes, Ernst & Young

Mr I Buchanan, Ms J Perry, Mr S Wren and Mrs C A Strutt, Nomura International PLC

Mr L Godenzie, Mr A Dewey, Mr M J Albert, Mr M Allan, Hogg Robinson PLC

Mr G Dresser, Accountancy Age

Mr V Watson, Clerical Medical Mr D Cherrill, Logica

Mr I Parkin, National Westminster Bank PLC

Mr G Colchester, Independent Consultant

Mr G Cox, South Somerset District Council

Eur Ing Lung, BAA PLC

Mr M J Lawson, Wimpey Group Services

Mr R Entwistle, Mardsen Building Society

Mr S Blair, Asda Stores Limited

Mr K McCormick, Poole Borough Council

Dr A Brookes, Independent Consultant

Mr K Parmer, Alexander and Alexander

Mr A Barker, Mr M Chowney, Mr P Martin and Ms F Wood, Cornhill Insurance

Ms H Millward, DTI

Mr D Bell, FMC

Mrs S Davis, Gloucester Constabulary

Mr M J Walker, Royal Insurance

It is very pleasing to be able to welcome so many new members. I hope to meet you in person at our technical briefing sessions - perhaps at the Internet session in January.

Membership statistics

We now have 414 members on our books although that number is likely to diminish. Members who have not renewed their subscriptions are due to be removed from our membership list. These non-paying members no longer receive the journal and pay the full rate if they attend technical briefing sessions.

By way of apology

Disaster recovery is so much part of the stock in trade of an auditor that there is a danger of complacency setting in. Why tackle disaster recovery again when there are so many more interesting projects to get on with? Internet for example; very topical, high risk, much more fun than good old DR. Even the least computer literate senior manager is aware that connecting to this `Internet' (whatever that may be) is a risky business and welcomes audit involvement.

For me, 1995 will be remembered as the year of the disaster. I will not bore you with the full story of the fire in my neighbour's garden that spread with remarkable speed to my hedge, fence, trees..... On the bright side, the firemen provided an unlooked for source of entertainment for the children and the fire missed the shed with petrol can, weedkiller etc. by a good 18 inches.

The burglary that greeted us when we returned home one summer day could be viewed as a further DR test. As in many modern households ours is a multi-computer household, `his and hers' portables from work plus our home PC - quite a haul. Having written countless pious comments on lack of backup, my own contingency arrangements were put to the ultimate test.....

Several weeks ago scenes of devastation greeted me on Monday morning. `Ram raiders' had visited over the week end and removed chips from nearly 70 machines. I would like to say that, like a well oiled machine, the DR plan swung into action. Perhaps that was not a totally accurate reflection of what actually happened. Let us just say that in reality, `opportunities for improvement' were identified.

Last week I had my most productive working day in goodness knows how long. The whole telephone system, internal and external, was out of action for 10 blissful hours. Countless in-trays and long postponed tasks benefitted throughout the whole organisation and E Mail came into its own. However, service to the public was not quite as usual.

Contingency planning has now taken on whole new level of significance in my life. More a ghastly reality than a theoretical possibility. Rather like a reformed smoker, I am in danger of becoming a DR bore but, remember, in the words of the Lottery 'it could be you'. Also like a reformed smoker, laspses into former bad habits are all too easy.

Take this issue of the journal. I had set aside time to write my contribution, admittedly just a little after the eleventh hour but, nonetheless, just within acceptable tolerance, when disaster struck. In the sort of nightmare scenario that most working mothers dread, both my children were struck down with the latest bug sweeping local schools. My washing machine stood the test, Dettol heads my shopping list and I have emerged to marvel again at the remarkable powers of recovery of the young....and to apologise most sincerely for the late delivery of my contribution which delayed this issue of the journal.

MEMBER PROFILES

Edited by Jenny Broadbent

If you have a suggestion for someone to be profiled please contact Jenny at her number in the Editorial Panel

GEORGE ALLAN

Current Position:
Senior Lecturer
Department of Information Science
Portsmouth University

CASG Involvement:
Academic Editor

George Allan is a computer professional through and through. He started as a Systems Analyst in the 1970s **before** studying formal structured programming techniques. An unusual approach, but one which lead to a deep and meaningful understanding of computer based information systems. In the 1980s, George became a project leader for the implementation of a small/medium size MIS at the Royal Naval Submarine School. Promotion to PM, found him responsible for the CBT pilot study implemented in six MoD establishments on the south coast of England. These successful implementations were followed with another project to completely overhaul and upgrade the computer support for a large company of scenario analysts. George took the company into the 20th century from a 512K System mainframe supporting 18 VDUs to the first passive-coupled cluster installed south of the Thames. The company emerged from the project 26 months later with 192 intelligent stations as nodes to the central cluster of 4 VAX machines. George concluded the project with a rolling plan for future enhancements and replacements over the company's next 3-5 years. He then moved into the world of academia to further his researches, write a book on project management and contribute to the academic press at large from his experimental learning/knowledge base.

George is a Chartered Engineer, a member of the Institute of Quality Assurance and a qualified TickIT Auditor. He is an active member of the British Computer Society as Vice-Chairman of the newly formed Configuration Management SIG, Secretary of the Hampshire branch of the Software Quality Group, an active contributor to PROMS-G and an examiner for the BCS paper 1 option in Systems Management, as well as the newly appointed Academic Editor of the CASG Journal. He is a member of MENSA and enjoys choral singing and playing golf when he gets time (which he says is never!).

ALAN OLIPHANT

Current Position:
Computer Audit Manager
The Standard Life Assurance Company

CASG Involvement:
Journal Contributor

Alan is a metallurgist who became fascinated by computers before he could find a real job. As a result, he has spent the last 22 years as a computer auditor, continuing to find new areas to keep him both interested and occupied. Since being given his first opportunity to dabble in the arcane science he has worked for a variety of companies across several continents with a rich mix of technologies.

Since 1986, he has worked with The Standard Life Assurance Company in Edinburgh and has concentrated on issues relating to systems software. Over this same period, he has been active with the Institute of Internal Auditors in both the UK and worldwide trying to promote the concepts of computer audit.

As he was awarded a fellowship of the BCS for his work in developing the concepts of computer audit, he feels that he needs to actually give something back. Hence his article in this edition of the journal which he sees as one small way of saying thank you to the BCS!

REPORT FROM THE MONEY BOX

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

There were no dramatic activities of a financial nature during the period. As of writing we have received annual subscriptions of approximately £3,000. A number of outstanding subscriptions are being chased and we hope to reach our subscription total of last year of approximately £5,000.

For our first technical briefing meeting in October we had 26 paying attendees generating revenue of £1,390. We had expenses of £1,850 and our current estimated loss for the day is £460. We issued our Autumn 1995 journal at a cost of £2,000.

We still have a healthy bank balance of approximately £27,000. As far as I am aware our Chairman has not received any suggestions on how the money could be purposefully used, as suggested in the Autumn 1995 journal. Please do not be shy, contact our Chairman if you have any suggestions.

BCS MATTERS

Colin Thompson
Director of Member Services

This column is edited by Colin Thompson, the BCS Membership Director, and focuses mainly on BCS news and events. The aim will be to keep readers in touch with what is going on in the BCS. and to provide background information and explanation where appropriate. Anyone with suggestions for particular issues to be covered in future editions should contact Colin at BCS HQ
(Tel: 01793 417410
e-mail: cthompson@bcs.org.uk).

The AGM

Amongst other things, the Annual General Meeting is the time for the Presidential change and the new BCS President, Dr Geoffrey Robinson, was installed by David Mann, the outgoing President, at the end of the 1995 AGM which took place on 25 October. Geoff is currently the head of IBM's Hursley Laboratory and his place as Deputy President is taken by Ron McQuaker who was the vice-president from 1991 to 1994.

The AGM also saw the appointment of a new Honorary Treasurer, Gerry Fisher, to replace Roger Baker who was standing down after 6 years in the seat. Gerry is Past President of the Society and this will be his second term as Treasurer.

One of the regular tasks for the AGM is the setting of the subscription rates for the coming year. The rates approved at this year's meeting are shown below, with the current rates shown in brackets. These rates will come into force in May 1996.

Fellow	£110 (110)
Member	£87 (84)
Associate Member	£68 (66)
Affiliate	£43 (42)
Student	£38 (37)
Companion	£80 (n/a)
Graduate	£38 (n/a)

The final two items on the list are new grades which are dependent upon the approval of the Privy Council and the subscription rates for those grades were approved on a contigent basis. Other elements of the submission currently under consideration by the Privy Council include the restoration of post nominal letters (AMBCS) to the Associate Member grade and the introduction of the chartered title 'Chartered Information Systems Practitioner' for Members and Fellows. We do not yet know when a decision on these changes to our Royal Charter will be made but we hope to have some more positive news early in 1996.

ISM RELEASE 3

The production of a new version of the Industry Structure Model has been the major project of 1995 and its launch will be an important event in the early part of 1996. For the benefit of those unfamiliar with the ISM, I should perhaps explain that it is a model of an organisation which represents, in matrix form, the streams of IS activity and the various levels of responsibility within those streams. By reflecting both the activity stream and the responsibility level, each of the cells in this matrix thus corresponds to a job within the IS organisation and each cell has a statement of the academic and experience requirements for that particular job.

The ISM is a unique product, not just within Information Systems, but across all the fields of engineering represented within the Engineering Council. It is central to the BCS Professional Development Scheme and provides a sound basis for structured training and development which is applicable to a wide range of organisations, both in the UK and overseas. By 1994 it was clear, however, that release 2, originally published in May 1991 was becoming outdated both in terms of its coverages and its presentation. Release 3 represents a major update of the model which has involved more than 150 volunteers in the task of writing and reviewing the new material.

ISM3 will differ from its predecessor in a number of important respects, including the fact that it is being created as a text database rather than as a document, and that the information will be related to roles, rather than jobs, within the IS organisation. Presentationally, the major difference will be that the model will be available as a PC based software product as an alternative to paper publication.

ISM3 is scheduled for release in February 1996 and further information may be obtained from the Professional Development Department at BCS HQ.

1995/6 RECRUITMENT CAMPAIGN

The other major campaign of 1995, the membership recruitment drive, continues to make progress and approximately 500 members have now volunteered to support by acting as the BCS contact point within their organisation and hold stocks of BCS literature. In many cases volunteers have also offered to make presentations to groups of potential members and a full presentation pack, including both OHP foils and speaking notes, has been distributed.

Major targets for the campaign include both the most senior and the more junior members of the profession and both groups are reflected in the business of Council at a recent meeting. The need for greater representation at the top end of the profession has been long recognised by the Society and the arrangements for the recruitment of senior IS professional has been considerably improved over the past few months. As a consequence, Council was able to approve invitations to BCS Fellowship for 27 senior practitioners at the meeting on 25 October.

At the same meeting Council also approved an amendment to regulations which will make it possible for the best

qualified candidates to achieve Associate Membership within 2 years of graduation rather than 4 years as at present. This change, coupled with those included in the Privy Council submission mentioned should provide a very much clearer path from student to full Member which should assist in the recruitment and, equally importantly, the retention of those coming into the profession.

Any suggestions aimed at improving recruitment and retention are welcome as also are more volunteers to support the recruitment activity within companies and universities.

ENGINEERING COUNCIL

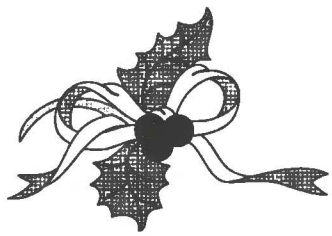
The relationship with the Engineering Council is one of the most important external links for the Society. Almost 7000 of our members now hold Chartered Engineer status and around 60% of our new applicants for professional membership now also qualify for the appropriate Engineering Council qualification.

This relationship with the Engineering Council has been the subject of extensive discussion over the past year as the Council conducted its 5 yearly review of our 'nominated' status. Given the fact the we had not satisfied one of the original requirements - that 50% of our Corporate Members should be Chartered Engineers by the end of 1994 - the outcome of that review was certainly not without doubt. However, the renewal of nominated status has now been confirmed and, whilst there are a number of conditions attaching to that renewal there is no repeat of the 50% requirement.

As many readers will know, the Engineering Council itself is currently undergoing major change which will have a significant impact on its relationship with the individual Engineering Institutions. The new Engineering Council is scheduled to come into existence on 1 January 1996 and I will include a brief outlines of the changes and the impact on the Society, in the next edition of this newsletter.

AND FINALLY.....

My very best wishes to everyone for Christmas and for a happy and prosperous New Year. I look forward to bringing you more BCS news in 1996.



Season's Greetings and a prosperous New Year to all our readers

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.*

The library holds several journals of interest to CASG readers. These include amongst others: Computers and Security, Computer Audit Update and Computer Law and Security Report. Conference proceedings from organisations such as the IEEE, IEE, BCS and ACM are also kept by the library. Some proceedings, but not all, are available for loan to BCS members. Photocopies of papers from proceedings and journals can be obtained from the Document Supply Service, a full bibliographic reference will be required.

Recent books added to the stock are listed below. These are all available for loan.

ISBN: 0-8186-3662-9
ABRAMS M D, JAJODIA S, PODELL H J
Information security: an integrated collection of essays.
IEEE Computer Society 1995

ISBN: 0-13-185596-4
STALLINGS W
Protect your privacy: the PGP user's guide.
Prentice Hall 1995

ISBN: 1-56592-098-8
GARFINKEL S
PGP: pretty good privacy.
O'Reilly 1995

SIZER R (ed.)
BRITISH COMPUTER SOCIETY
Security guidelines in information technology for the professional practitioner: the computer law and security report special supplement.
Elsevier Advanced Technology 1994

MICHAEL J
Privacy and human rights: an international and comparative study, with special reference to developments in information technology.
Dartmouth and UNESCO 1994

ISBN: 0-201-55805-X
NEUMAN P G
Computer-related risks.
Addison-Wesley and ACM 1995

1-85554-352-4
DEVARGAS M
The total quality management approach to IT security.
NCC Blackwell 1995

ISBN: 0-11-886137-9
AUDIT COMMISSION FOR LOCAL AUTHORITIES
Opportunity makes a thief: an analysis of computer abuse.
HMSO 1994

ISBN: 0-13-305541-8
AMOROSO E G
Fundamentals of computer security technology.
Prentice Hall 1994

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

REFEREED ARTICLE

Estimating Software Development Time & Costs

George Allan

Abstract

This paper, which comprises three parts, aims to introduce and explain a process for software estimating. It is anticipated that this will provide auditors, software engineers and project managers with an insight to a stable method for estimating time, cost and staffing requirements. The basic model distinguishes between three different development modes - Organic, Semi-detached and Embedded. These are explained and worked examples are included to illustrate the theoretical points.

Further refinements to the model allow estimates to be made for more detailed partitioning of the development cycle. This paper discusses the time, cost and staffing requirements for Product Design, the actual Programming and the Integration & Testing of software units. A further consideration sub-divides the actual programming into its two realistic components of Detailed Design and Coding. Worked examples throughout are progressive in difficulty as each point is illustrated and accumulated into the auditor's/software engineer's/project manager's tool kit.

Key Words

Software estimating; CoCoMO; Person months; Development time; Development cost; Organic mode; Semi-detached mode; Embedded mode; Product design; Programming; Integration & Test; Detailed design; Code & unit test.

Part 2 of 3

FURTHER REFINEMENTS

So far our estimates have been of a global nature and dealt only with overall Effort and overall Development Time, treating the whole software development as a single "black box" unit. The next step is to consider the software development in more detail with thought to the actual phases involved. Once a specification is received (from the Analyst/Designer for traditional life cycle development, or as a technical specification derived by the Analyst/Programmer and User as part of a prototype, or whatever other authority) there are 3 main phases to consider in turning this authorised requirement program specification into the deliverable product of a software unit. The overall software unit is now considered as being comprised of 3 main phases.

These 3 main phases are:

i. Product Design

ii. Programming

iii. Integration and Testing

Of the overall Effort calculated from the basic CoCoMo formula we now consider what percentage of this overall effort will be spent by the professional programmer on ***Product Design***; then the percentage of Effort for actual ***Programming*** and finally the percentage of Effort for ***Integration and Testing.***

Product Design Phase

Having received a specification, the first task for the programmer is to sit down and design the software to accomplish the required result. This phase will include the logical structure and initial documentation to achieve this end. In prototyping it could include the design of the basic structure, screen layouts, colour schemes. It should be done in close harmony with the User so that the final product is what was ordered and ***"does not result in any surprises at all"***. This will take 16%, 17% or 18% of the overall effort depending on development mode as we shall see.

Programming Phase

When the design is complete there will then be the actual programming phase which will take between $^1/_2$ and $^3/_4$ of the overall effort. The percentage will actually vary from 48% up to 68% and depends on the development mode and the actual size of the software unit in KDSI.

Integrating & Testing Phase

Finally, once the unit has been completely coded it must now be Integrated and Tested with other software within the project. This is a test of such facets as interfaces, how our Software Unit is going to react and inter react with other Units both at interfaces, passing of parameters and variables, calling routines and boundary conditions. The actual test harness is beyond the scope of this particular text. The amount of the original overall Effort varies from 16% to 34% depending on development mode and the actual size of the code to be Integrated and Tested.

The above percentages are tabulated as follows:-

Table 2 : Effort Distribution

Mode	Phase	Small 2 KDSI	Intermediate 8KDSI	Medium 32 KDSI	Large 128 KDSI	Very Large 512 KDSI
ORGANIC	Product Design	16	16	16	16	—
	Programming	68	65	62	59	—
	Integration & Testing	16	19	22	25	—
SEMI-DETACHED	Product Design	17	17	17	17	17
	Programming	64	61	58	55	52
	Integration & Testing	19	22	25	28	31
EMBEDDED	Product Design	18	18	18	18	18
	Programming	60	57	54	51	48
	Integration & Testing	22	25	28	31	34

For each given development mode in the above table - for any given size of software unit note that the total effort adds up to exactly 100%

Worked Examples

We will now use the original 2 formulae from Table 1 and the Effort Distribution within the 3 main phases from Table 2 to work a number of examples.

Example 5

Consider a Software Unit of 8 KDSI being developed in Organic Mode.

Estimate the overall Effort needed and break this into the 3 phases:-

a) Product Design

b) Programming

c) Integration and Testing

First step is to estimate the overall Effort required in person months from the basic CoCoMo formula (given in Table 1).

We are told that this software unit is being developed in Organic Mode.

Required effort
in person months
= PM = $2.4\ (KDSI)^{1.05}$ person months

$= 2.4\ (8)^{1.05}$ person months

$= 2.4 \times 8.88$ person months

= 21.3 person months of effort

Next step is to consider how this total Effort is divided amongst the three phases. From Table 2 we use the Organic Mode section and the column for size 8 KDSI. We see the percentage distribution of Effort is:-

	%	Effort Distribution
Product Design	16	$\frac{16 \times 21.3}{100} = 3.4$ person months
Programming	65	$\frac{65 \times 21.3}{100} = 13.9$ " "
Integration & Testing	19	$\frac{19 \times 21.3}{100} = 4.0$ " "
	100	21.3 person months of effort

CONCLUSIONS

An ORGANIC MODE software unit of size 8 KDSI will require 21.3 person months to develop of which:

- *3.4 person months will be in Product Design*
- *13.9 person months will be in Programming*
- *4.0 months will be in Integrating and Testing the Unit*

Example 6

Consider a software unit of 32 KDSI being developed in Semi-Detached Mode [small but probably complicated]. Estimate the overall Effort needed and break this into the 3 phases.

Step 1

As before, use Table 1 to estimate the effort for Semi-Detached Mode.

Required Effort
in Person Months
= PM = 3.0 $(KDSI)^{1.12}$ person months

Size is 32 KDSI
PM = 3.0 x $(32)^{1.12}$ " "

= 3.0 x 48.5 " "

= 145.5 person months of effort

Step 2 from Table 2 the division of effort for Semi-Detached Mode and size 32 KDSI:-

	%	Effort
Product Design	17	$\frac{17}{100}$ x 145.5 = 24.7 person months
Programming	58	$\frac{58}{100}$ x 145.5 = 84.4 " "
Integration & Testing	25	$\frac{25}{100}$ x 145.5 = 36.4 " "
	100%	145.5 person months

CONCLUSIONS

A SEMI-DETACHED MODE software unit of size 32 KDSI will need 145.5 person months of Effort to develop of which:

- *24.7 person months will be in Product Design*
- *84.4 person months will be in Programming*
- *36.4 person months will be in Integrating and Testing the Unit*

Example 7

A software unit of 512 KDSI is being developed under the most difficult of conditions, therefore we use the Embedded Mode. Estimate the overall Effort needed and break this into 3 phases.

Step 1 Estimate overall effort using Table 1 for Embedded Mode.

Required Effort in
Person Months
PM = 3.6 x $(KDSI)^{1.20}$ person months

= 3.6 x $(512)^{1.20}$ person months

= 3.6 x 1782.9 person months

= 6418.4 person months of effort

Step 2 from Table 2 division of effort is:-

	%	Effort
Product Design	18	$\frac{18}{100}$ x 6418.4=1155.3 person months
Programming	48	$\frac{48}{100}$ x 6418.4 = 3080.8 " "
Integration & Testing	34	$\frac{34}{100}$ x 6418.4 = 2182.3 " "
	100%	6418.4 person months

CONCLUSIONS

An EMBEDDED MODE software unit of size 512 KDSI will take 6418.4 person months of Effort to develop of which:

- *1155.3 person months will be in Product Design*
- *3080.8 person months will be in Programming*
- *2182.3 person months will be in Integrating and Testing the Unit*

There is a similar, though not exactly the same, division of the scheduled time distribution for TDEV. The corresponding division of time among the 3 main phases is known as the ***Schedule Distribution*** and is given in Table 3.

The **first step** is to use the TDEV formula from Table 1. Be careful to use the correct development mode either Organic, Semi-Detached or Embedded. The formula requires the Effort in PM which you will have calculated previously.

This will result in an overall development time TDEV in months.

The **second step** is to Schedule the Distribution of this overall TDEV as shared among the 3 main phases - ***Product Design, Programming, Integration and Testing.***

This we do from **Table 3.**

Table 3: Schedule Distribution of TDEV

Mode	Phase	Small 2KDSI	Intermediate 8 KDSI	Medium 32 KDSI	Large 128 KDSI	Very Large 512 KDSI
ORGANIC	Product Design	19	19	19	19	—
	Programming	63	59	55	51	—
	Integration & Testing	18	22	26	30	—
SEMI-DETACHED	Product Design	24	25	26	27	28
	Programming	56	52	48	44	40
	Integration & Testing	20	23	26	29	32
EMBEDDED	Product Design	30	32	34	36	38
	Programming	48	44	40	36	32
	Integration & Testing	22	24	26	28	30

Worked Examples

Let us reconsider examples 5, 6 and 7 with regard to TDEV.

Example 5a

First step is to estimate the Total Development Time required in months from Example 5:-

Required effort
in person months =
PM = 21.3 person months .....from Example 5

From Table 1
TDEV = $2.5 (PM)^{0.38}$ ..... for Organic Mode Development

= $2.5 (21.3)^{0.38}$ months

= 2.5 x 3.28 months

TDEV = 8 months development time

Next step is to consider how this total Development Time is divided amongst the 3 phases. From Table 3 we see the Schedule Distribution of this time is for a software unit of size 8 KDSI in Organic Mode:-

	%	Effort
Product Design	19	$\frac{19}{100} \times 8 = 1.5$ months
Programming	59	$\frac{59}{100} \times 8 = 4.7$ "
Integration & Testing	22	$\frac{22}{100} \times 8 = 1.8$ "
	100%	8.0 months

CONCLUSIONS

An ORGANIC MODE software unit of size 8 KDSI will take 8 months to develop of which:

- *1.5 months will be in Product Design*
- *4.7 months will be in Programming*
- *1.8 months will be in Integrating and Testing the Unit*

Example 6a

First step is to estimate the Total Development Time required in months from Example 6:-

Required effort
in person months =
PM = 145.5 person months

From Table 1
TDEV = $2.5 (PM)^{0.35}$ for Semi-Detached Mode development

= $2.5 (145.5)^{0.35}$ months

= 2.5 x 5.7 months

= 14.3 months development time

Next step is to consider how this total Development Time is divided amongst the 3 phases.

From **Table 3** we see the Schedule Distribution of this time for a unit size of 32 KDSI is:-

	%	Effort
Product Design	26	$\frac{26}{100} \times 14.3 = 3.7$ months
Programming	48	$\frac{48}{100} \times 14.3 = 6.9$ "
Integration & Testing	26	$\frac{26}{100} \times 14.3 = 3.7$ "
	100%	14.3 months

CONCLUSIONS

A SEMI-DETACHED MODE software unit of size 32 KDSI will take 14.3 months to develop of which:

- *3.7 months will be in Product Design*
- *6.9 months will be in Programming*
- *3.7 months will be in Integrating and Testing the Unit*

Example 7a

First step is to estimate the Total Development Time required in months from Example 7:-

Required effort
in person months =
PM = 6418.4 person months

From Table 1
TDEV = $2.5 (PM)^{0.32}$ months
= $2.5 (6418.4)^{0.32}$ months
= 2.5 x 16.5 months
= 41.3 months development time

Next step is to consider how this total Development Time is divided amongst the 3 phases. From **Table 3** we see the Schedule Distribution of this time is:-

For size 512 KDSI in Embedded Mode:-

	%	Effort
Product Design	38	$\frac{38}{100} \times 41.3 = 15.7$ months
Programming	32	$\frac{32}{100} \times 41.3 = 13.2$ "
Integration & Testing	30	$\frac{30}{100} \times 41.3 = 12.4$ "
	100%	41.3 months

CONCLUSIONS

An EMBEDDED MODE software unit of size 512 KDSI will take 41.3 months to develop of which:

- *15.7 months will be in Product Design*
- *13.2 months will be in Programming*
- *12.4 months will be in Integrating and Testing the Unit*

Average Staff Required In Each Phase

Now we are in a position to calculate an estimate of the average number of staff required *for each of the three* main phases. As before the means of calculating the required number of staff is:- $\frac{\text{Effort}}{\text{Duration}}$

For each Phase the average number of staff required =

$\frac{\text{Phase effort in person months}}{\text{Phase Person Months}}$ =

$\frac{\text{Phase duration in months}}{\text{Phase Months}}$ = persons

Example 5b

So considering examples 5 and 5a we have staffing requirements.

Product Design	3.4/1.5	=	2.3 staff
Programming	13.9/4.7	=	3.0 staff
Integration & Testing	4/1.8	=	2.2 staff

The original overall estimates would have an average staff of

$\frac{\text{Effort}}{\text{Duration}} = \frac{21.3}{8}$ = just over 2.5 people.

Example 6b

So considering examples 6 and 6a we have staffing requirements.

Product Design	24.7/3.7	=	6.7 staff
Programming	84.4/6.9	=	12.2 staff
Integration & Testing	36.4/3.7	=	9.8 staff

Compare this more refined position with an original estimate of $\frac{145.5}{14.3}$ = about 10 people.

Example 7b

So considering examples 7 and 7a we have staffing requirements.

Product Design	1155.3/15.7	=	74 staff
Programming	3080.8/13.2	=	233 staff
Integration & Testing	2182.2/12.4	=	176 staff

Compare with overall average of $\frac{6418.4}{41.3}$ = 155 staff.

Summary so far:-

From the original first cut estimates of Effort and Duration, we should now have a better idea of:

Required staffing levels.

A basic Estimate of Costs.

Staffing Tasks within Phases.

More credible estimates than merely global figures.

End of Part Two of Three - To be continued in the next edition

George Allan is a Senior Lecturer in the Department of Information Science at Portsmouth University.

BOOK REVIEW

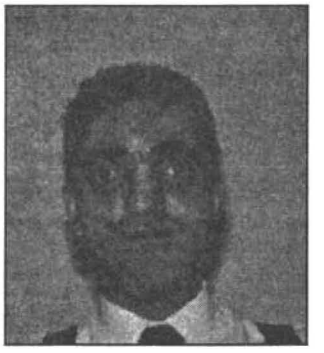
This column is edited by Iltaph Khaliq who would like volunteers to help him with the review process. If you are interested please contact Iltaph at the number provided in the Editorial Panel.

TITLE:	FINANCIAL TECHNOLOGY Effective Cost Management
AUTHORS:	James Essinger
PUBLISHER:	FINANCIAL TIMES Financial Publishing
ISBN:	ISBN 1-85334-226-2
PRICE:	UK Price : £215.00
PAGES:	109 pages

This management report is presented as "An essential guide for Senior Managers". The report is split into two parts; Part 1, Cost Effective Ways of Setting Budgets and Assembling the Requisite Human Resources and Part 2, Cost-Effective Management of the System Development Life Cycle.

Within Part 1, Chapter 1 explains "The Role of Technology in the Financial Sector". Thirteen pages of background information are summarised quite succinctly in the chapter's conclusion which comprises three paragraphs. Subject to the final comments made in this review, this particular chapter might well prove useful to a new entrant to the Financial Services sector.

Chapter 2 is entitled "Budgeting Financial Technology". I felt that there were several missed opportunities here. Whilst talking about a hierarchical budget approval system and the need for making out a business case, there were no illustrations, suggested contents or examples of a good proposal. There are many subjective or qualitative arguments in this chapter, without the provision of any evaluative methodologies or quantitative measures.



Chapter 3 covers "Cost Effective Assembly and Management of the Financial Technology Team". The six pages provide an overview of Human Resourcing issues.

Chapter 4 is entitled "Using Technology Consultants and Systems Designers Cost Effectively". These five pages conclude Part 1 and outline the drawing up of Terms of Reference, having decided whether to design an application in-house or contract-out.

Part 2 outlines the Systems Development Life Cycle. In 65 pages and 10 chapters, it provides an overview in very broad terms. Chapter 5 is entitled "Preliminary Planning", Chapter 6: "Production of the Feasibility Study", Chapter 7: "Analysis of the Application Requirements of the New System", Chapter 8: "Definition of the System's Precise Functions", Chapter 9: "Planning the Technical Design", Chapter 10: "Selection of Vendors", Chapter 11: "Design and Construction of the System", Chapter 12: "Testing", Chapter 13: "Implementation" and finally, Chapter 14: "Maintenance and Support".

Final Comment

Highly overpriced for what it is, wholly inadequate for its stated market, voluminous for its actual content. I personally would use the same amount of money to stock my bookshelf with half a dozen books that would prove substantially more useful.

The following article, received via my bedroom window in the early hours of the morning, appears to be an account of an auditor in a foreign land. Some of the manuscript was difficult to decipher due to the paper having been used, based on the smell, to wrap a very strong and runny cheese. At least that is what I hope it was used for! Read on and learn that the grass is not always greener on the other side of the pond (expletives deleted). If any of you out there have a an auditing experience that you would like to share with your colleagues, anonymously if necessary, then send it to me at the editorial address, not via my bedroom window. A bottle of bubbly at the end of our current season to the best contribution, as decided by me. Ed.

HOME AND AWAY

(or how the audit team learned that it's better to arrive than to travel hopefully)

M. Herrison

Having spent years working in the home environment with very much the same faces and issues, such as work pressure to finish the job and get things out (which always come to a grinding halt at the bottle neck called management review), we looked forward to a new adventure.

Audit in a foreign subsidiary. Part financial, part operational. A real challenge.

Careful planning, preliminary visits, plenty of cash what could go wrong?

Well this is how it went.

Take the 'chunnel' it's quick, better than the ferry, which is out of date and slow; your tickets will be waiting for you - they said !

We arrived at Folkestone in two cars, four people: two young ladies two 'slightly' older men. Pass through the first ticket barriers and get sent down a diversion to a porta-cabin. Park the car, enter cabin, quote transport order number, get ticket, return to car, drive half a mile to find duty free. Buy duty free return to car.

Drive around for a while through ticket barrier and passport control and !!!! French security take instant dislike to female colleagues. Car taken to one side, girls out, white gloves on. Oh S**t, now what thinks I?

TML staff desperately trying to get me to join queue for chunnel. Me insisting that I am waiting for colleagues. Told to wait behind screen! While wondering what to do security arrive and tell me get round here if I am with the ladies! Oh S**t, again.

Phew! Relief, white gloves are to run over vehicle surface then analyse for semtex and other substances. Girls allowed to leave, told to go too. Phew!

While all this goes on two trains have gone. What price the shuttle now?

After that it got better. Found our way in record time, nice food, nice company, plenty to drink.

Of our number, two can speak very good French. Another can order a beer (Oi Garcon dos cereva por favor) and the other can point at a beer.

Week One. Preliminary meetings with management at the head office. Begin all meetings with assumption that they don't speak English (I recommend it), within five minutes they will be proud to inform you in perfect English that they actually do speak a bit !

After one such session, when accompanied by a colleague from England who had been working in France on and off for two years, this chap put his hand on his hips and came out with 'well b****r me. I've been here two years and he never told me that he could!' Just goes to show.

Well in the first days of review a few eye openers appeared.

Why don't the French have a word for security? I mean, security as safety is all very well and I appreciate a good socialist society as much as anyone, but safe files are not the same as secure ones. I digress, at a site supposedly secure it was seen that the fire exits were not alarmed, so during trading anyone can enter or leave by the back door without passing through the sales area. The management said, 'no they can't, the fire exits are locked '!

Well, so to the hotel. Yes! It's got a bar, but oh how sad, one beer 15 Ffr (two quid) and a small beer at that. (After a few it doesn't seem to matter much though).

Evening meals were (usually) a treat. A different restaurant every night, different wines, different cheeses.

Our food consumption became almost a local legend (Okay, it wasn't the food consumption that was legendary, but close).

We ate anything offered, most of the time. I had to draw the line at l'escargot (they look like snails) and even the most francophile amongst our number wouldn't go the whole way with grenhuilles.

I have tasted my first oysters (now addicted), but nearly lost the first lot. Two of us were trying them for the first time in a fine sea food restaurant and with the lemon and lots of vinegar they were slipping down quite

well thank you until ! Oh yes there is always one! Are you sure they are alive she said? Que, we countered, alive? Oh yes, they should be alive. You can tell when you put the vinegar or lemon juice on them they sort of shrink. They did! I have to say that as a main course that day I had skate wing and capers. Delicious. (We had to go back and have it again, couldn't stand the thought of a poor skate swimming around in circles for ever).

Fromage: one evening at a restaurant (Michelin recommended) when the waitress opened the cover of the cheese board all the flies flew away! The Roquefort was virtually chasing them off. I think that's the place we had a cheese, whose name I still don't know, that was presented looking like a small volcano: cone like and red on the outside. Tres fort said the girl only serving a sliver. Well in that case, as a man who knows stilton can see any cheese off, give me a big bit. Tres fort it was. It's how they sell more after dinner wine, I think.

Well our days continued, finding that in France control and weakness are synonymous for the same thing and that procedures are always being put together for the next time you come. Did you know that no one has a works canteen or staff restaurant and everyone goes home for two hours at lunch time! Well they did while we were there.

Lunch times became a route for pleasant experimenting with various dishes. Salads proved safest. Why, oh why, do they serve chips with everything, except fish of course!

Roll on Friday and back to Blighty beginning to feel like the expeditionary force.

Hit the M20. No prob. M25 - Whoops where did all this traffic come from? Don't they know we've been flying the flag?

Monday: back to France. New hotel this week. Central point for us all as we are working in groups in different places.

Arrive at new hotel in dark (followed a UK registered Discovery twice round the town. Idiot! I thought he knew were I was going).

Book in. What is this? It's a cross between a social security B & B and a Calcutta brothel. *(Now how does he know that? - Ed).* I check in. Am told by the 'madame' that I am Ms X and I can't possible be me as I am there already! Go to room (sorry broom cupboard), leave best suit squashed in suitcase, as squashed in suitcase is cleaner than wardrobe. Go to look for colleagues, surely in a bar?

Ah, Ah! Here they are looking lost standing in town square. What's to do? What's your room like they demand? Well, I've slept in better ditches in my youth, I respond. Can't be as bad as ours, they reply. We go to see mine. Sorry, they apologise. At least there are no mice droppings in ours. Tired we decide to give it a go and look for somewhere to eat. You've got to be joking. This town is closed and has been for years as far as I could see.

Eventually found a cafe/bar that looked okay, but sadly that was the night Red Rum had died and we hadn't meant to eat him. One colleague doesn't eat all her food and gets a lecture from the bar owner who definitely (despite looking like a corpse) thought that with Gallic charm he was in with a chance (he didn't appear to be bothered by which sex either). Made our excuses and left.

Return to hotel, out with Michelin (in fairness to them this hotel is not in their guide any more) and ring where we were the week before to book for rest of week.

And so to bed.... Three friends now in another building with both sets of car keys. Yours truly alone in old part of strange hotel. Due to ample beer/wine straight to sleep (approx. 11.30.) Midnight, 30 minutes later battle of Waterloo in corrida, or for the Spanish among you a corrida in the loo, I don't know which.

Now wide awake. Door knob tried more than once from outside. Put TV on. Now I know why porn in France isn't blue it's rose. Once you've seen some of it your eyes go red (Yes, I said eyes).

Read a book that I had brought to last the week. Very hot in here. Open window - b*****ks, the hotel is next to an abattoir, I think, as it's the only explanation of the smell. Shut window.

Buzz, buzz. Ouch! Oh No, the room is full of mosquitoes. Now what? Go to bathroom which is through the wardrobe, well sort of anyway, put light on in WC which is through the bathroom hope light will attract the insects away from main room.

If only I had the car keys I could kip in the car. Around 5.30ish fall asleep. Sixish, dust cart in street. S*d it, get up.

Do you know that although being booked in for a week the lady (!) at reception wasn't a bit surprised when we all booked out. It was at this point that we sustained an injury! Blamed on quality of hotel we suffer a drop-out with a bad back. Home to his physio.

Three left. Regardless we continue.

Boss comes to see us and review progress. Take her to lunch at a moderately expensive restaurant. I pay. Going back to car, having just paid nearly twenty quid each for a salad and one beer, which she didn't drink, she come out with a classic. 'It really isn't as expensive as people think it is'.

On that subject, now that colleague with bad back has left, I get the wine list with every meal (I can cope with that), but I also get the bill! Innocently, I think it's because the French are sexist and always assume that the man is paying (three weeks cash advance from the company runs out in four days).

When back home I explain to the wife why I have no money. She puts it all into perspective (pricks balloon actually). She explains that it is due to the age difference, the waiters, etc., think that I am taking my daughters out for a treat! Thanks dear.

Life goes on.

Getting to know the score now. At the office there are two main sources of coffee. One in the posh bit, two Ffrs a time for decaf. One in the warehouse, scruffy area, only 1 Ffr.. It may not be coffee but it is strong!

On bonjour terms with everyone, as everyone else is with everyone else too.

Have noticed with the kissing. Only the nice girls get kissed and then only by other girls.

Toilets a bit odd. There are no men's toilets. Starting to get used to it. Have to watch out back home that I don't get done for going to the wrong one.

One colleague, definitely a potential terrorist, stopped by customs men in the middle of road nowhere near a border, still 30 miles from Calais! Had a chat, discussed not a lot and demanded salt and vinegar crisps as a bribe. Bizarre!

Another week passes.

Use the ferry now. It's much more civilised. P & O club class, soft drinks and beverages free, steward service, English papers on return journey (have you noticed, it's the same on international flights, they never have the Sun or the Daily Mirror? How do they keep up with the racing results?).

Well, must sign off for now I'll let you know more from the other side when the follow ups and reports have been issued to report on how they take it and if anything gets done as a result.

A Bientot.

M. Herrison
(Mr Hedgehog)

Some people suffer from 'finger' trouble, others suffer from 'brain deficiency'. It's not very often that you hear of someone who has both!. Ed.

There seems to be a positive correlation between the degree of stupidity of an end-user and his or her seniority. So it was not in the least surprising to hear at last week's Data Warehousing '95 conference from a speaker who recorded a top manager totally confounding the IT department.

The exchange went like this:

Very senior manager (VSM): This system doesn't work.

IT: What's gone wrong?

VSM: My screen has come up saying something incomprehensible, and then it said, "Press any key."

IT: Er, ye-es. So what's the problem?

VSM: There's no bloody "any" key on this damn keyboard!

from Computer Weekly, 30th November 1995

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 June to the following May each year)

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

CORPORATE MEMBERSHIP (Up to 5 members)* £75

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

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

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

BCS membership number: _____

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

Educational Establishment: _____ £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)

British
Computer
Society

Management Committee

CHAIRMAN	Alison Webb	Independent Consultant	01223 461316
SECRETARY	Raghu Iyer	KPMG	0171 311 6023
		Email: raghu.iyer@kpmg.mark400.gb	
TREASURER	Bill Barton	BSkyB	0171 705 6821
MEMBERSHIP SECRETARY	Jenny Broadbent	Cambridgeshire County Council	01223 317256
JOURNAL EDITOR	John Mitchell	LHS - The Business Control Consultancy	01707 851454
		Email: jmitchell@lhs.win-uk.net	
MEETINGS	Paul Howitt	Tesco Stores Limited	01992 644250
	Jim Ewers	Hertfordshire County Council	01992 555328
	John Bevan	Audit &Computer Security Services	01992 582439
	Geoff Wilson	Independent Consultant	01962 733049
	Allen Brown	Independent Consultant	01803 327874
	Diane Skinner	Audit Commission	01179 236757

Membership Enquiries to:

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

Tel: 01223 317256

casg
Computer Audit Specialist Group

Presents

Information Highways:

The Opportunities for Good and ILL

Tuesday 16 January 1996
9.30 am for 10.00 am at
The Royal Aeronautical Society,
4 Hamilton Place, London W1V 0BQ

British Computer Society

The second of our full-day technical briefings. This one reflects on the opportunities for good and ill which currently exist both on the internet and on more local routes! It includes the expanding role of the "traffic policeman", as the day also considers the audit and security issues surrounding electronic mail and telephone systems.

This is an unrepeatable and very affordable chance to see a demonstration of E-Mail and the World Wide Web, and to hear from top-class speakers and fellow professionals about aspects of communication which we ALL may now need to consider in our everyday working and leisure lives.

Registration Procedure

The fee for the day, which includes conference papers, coffee, lunch and tea is £40.00 (net of VAT; gross £47.00) for members of the following organisations:-

BCS, CASG, CIPFA, ISACA, ICAEW IT Faculty

The fee for non-members is £140.00 (net of VAT; gross £164.50)

A Registration Form is enclosed with this issue of the Journal. The non-member fee includes the cost of Corporate Membership of the Computer Audit Specialist Group for the season 1995/96, so please complete the membership form on the back of the Registration Form.

Individual non-members will be accepted at the member rate if they also enrol as CASG members at the same time, using the membership application form on the reverse of the Registration Form.

Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ