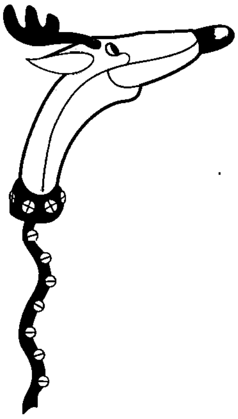
ISSN 0961-9348

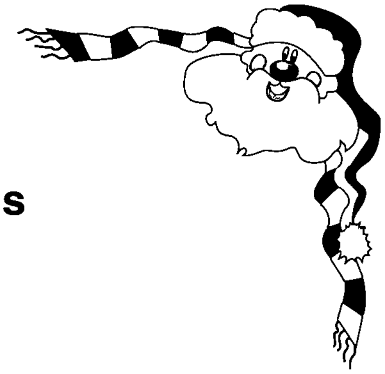
casg
Computer Audit Specialist Group

JOURNAL

VOLUME 11 NUMBER 1 WINTER 2000

The British Computer Society





Programme for members' meetings 2000/2001 season

16th January 2001	**Phone Fraud** *Telecommunications related fraud has fast become a major threat in today's world. Everyone from the largest corporation to the teenager with a mobile is at risk from attack. How can you reduce the risk?*	Evening 16.00 for 16.30 KPMG
13th February 2001	**Implementing PKI** *Public-key infrastructure (PKI) is the combination of software, encryption technologies and services that enable enterprises to protect the security of their communications and business transactions on the Internet. We will focus on the practical aspect of implementing PKI.*	All Day 10.00 to 16.00 Royal Aeronautical Society
15th May 2001	**WAP Security** *The massive growth in the popularity of mobile phones, personal digital assistants and handheld PCs is a huge new market for anyone involved in e-commerce. We look at the security offered with WAP solutions.*	Evening 16.00 for 16.30 KPMG

The late afternoon meetings are free of charge to members.

For full day briefings a modest, very competitive, charge is made to cover both lunch and a full printed delegate's pack.

For venue maps see page 24.

Contents of the Journal

EDITORIAL

I am now ADSL enabled. Having a permanent and very fast (500 kbyte/second) link to the Internet means that I can indulge in that idiosyncratic web browsing which often turns up real gems of information, such as the 79,350 hits on the word 'hatching' when I was really interested in 'hacking'. Very interesting stuff it is too. It's nice to know that there are people out there who are even more weird than computer auditors. Web cams to spy on the birth of Clarissa the duck's siblings, must be exciting to someone, I suppose, but the use of lasers in the process is positively indecent.

The link has not been without its teething problems, such as the 5 days of non-operation just hours after it had been installed, but why kick BT when they are already down? I have also yet to sort out my e-mail connectivity to make full use of the link, but I suspect that is simply a question of shelling out more money to some cash strapped dot.com somewhere in the ether. However, having read Valji and Chadwick's paper on e-mail security, which you will find in this edition, I am not sure that I should bother. Woody Allan once said 'just because you're paranoid, doesn't mean that they are not out to get you'. Having been permanently linked to the Internet for just a short amount of time, I am absolutely convinced that 'they' are out to get me. My firewall pings with alarming frequency to inform me that it has detected yet another attempt to probe my perimeter, but of equal concern is its constant detection of ***my*** browser trying to access sites on the internet without my knowledge. It appears that many sites in my favourites folder seem to think that they have an implied right to whiz off to their home sites whenever they get the opportunity and without a by your leave sir. I know that they are probably trying to be helpful by looking for updates, but I find it extremely disturbing, especially as some of the attempts relate to sites that I have never book marked. I suspect it is something to do with those little cookies that come down the wire every time one stops at a site for even a few seconds.

Apart from Valji's paper we have an article on QiCA by David Chadwick which complements the information provided by the IIA; an overview of changes in SAP R/3 by Bob Ashton; a bulletin on interesting web sites from Andrew Hawker and the usual update on our parent body by Colin Thompson. We also have a plea from Caroline Smith for help with her MBA dissertation in information security. Please spend a few minutes to speak to her. Remember the IIA's motto of 'progress through sharing'? Well, do some sharing with Caroline.

You will also find our regular cartoon competition. Give it a try. I like the dark evenings to be lightened by the occasional burst of humour.

The compliments of the season to you all and a happy and prosperous new year.

John Mitchell

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

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
Email: john@lhscontrol.com

Designed and set by Carliam Artwork,
Potters Bar, Herts
Printed in Great Britain by PostScript,
Berkhamsted, Herts.

E-Mail Security: Establishing Solutions for the Communications Tool within Academic and Organisational Environments

M.K. Valji and D.R. Chadwick
Information Integrity Research Centre,
School of Computing & Mathematical Sciences,
University of Greenwich, London SE10 9LS, UK
svalji@talk21.com, cd02@greenwich.ac.uk

1. Introduction

The advent and the rapid evolution of e-mail has been to the advantage of organisations and academic institutions within their respective environments; allowing for efficient and effective communications which has ultimately altered the way in which entities such as vendors, customers and business partners communicate with each other.

However, the technology to manage and monitor e-mail has not developed in unison with the increased use and volume of e-mail traffic over the Internet. Without the tools required to re-claim back the control of e-mail infrastructures, organisations and academic institutions face increasing risks in protecting their information systems security and maintaining e-mail security.

This paper will examine the fundamental issues encompassing e-mail security; it will look at practical implications of e-mail security and focus on problems that can arise through the utilization of e-mail. Feasible recommendations will then be provided for these problems as well recommendations for the academic and organizational environments.

To commence, this paper will determine the general area of Information Security within which e-mail is incorporated, once this has been ascertained e-mail security in general will be assessed. The paper will then progress on to the practical implications of e-mail security.

2. Information Systems Security

The speed of technological advancement and innovation, combined with the growing needs and dependencies being placed on such accelerated growth, has developed information security into one of the most imperative and integral elements in IT. Another critical factor placing further emphasis on information security is the distributed ethos of computing nowadays and the need for organisations to share and distribute information.

Information security is a holistic function that encompasses security in both physical and technical terms, it affects virtually all businesses and a recent DTI (1997) survey showed that 90% of all organisations questioned reported at least one breach, with an average cost of £16,000. Within the business environment information security should be integrated as part of an organisation's strategic goals and objectives and, if effective, should ensure that these goals can be met and maintained.

The extent to which information security is considered or implemented is dependent on the context or situation within which information or an information system is used. In its simplest form information security can be seen within the home, e.g. ensuring deeds and insurance documents are kept safely so that they are available when required. However, within the business environment, having the right information at the right time can make the difference between profit or loss, success and failure. Effective information security will help control and secure information from inadvertent or malicious changes and deletions or unauthorised disclosure (DTI 1997).

2.1 BS7799: Code of Practice

The most effective way of providing information security is to use a structured approach based upon an organisation's specific security requirements. A widely recognised structured approach is the 'Code of Practice for Information Security Management' which was published in 1995 as a British Standard (BS 7799).

The standard provides a comprehensive set of security controls comprising the best information security practices in current use. The standards objective is to provide organisations with a common basis for providing information security and to enable information to be shared between organisations.

BS7799 encompasses many controls and identifies ten that are considered 'key controls'. Organisations should consider the implementation of the ten 'key controls' as a security baseline across the organisation. These 'key controls' do not have to be adhered to explicitly and additional measures and controls can be added depending on the business area.

The Ten Key Controls

- Information Security Policy Document
- Information Security Education and Training
- Virus Controls
- Control of Proprietary Software and Copying
- Data Protection
- Allocation of Information Security Responsibilities
- Reporting of Security Incidents
- Business Continuity Planning Process
- Safeguarding of Organisational Records
- Compliance with Security Policy

2.2 Security Policy

The security policy is possibly the most important security document an organisation requires. An effective policy that is created using the appropriate methodology should lead to information security being seen as a business enabling technology. An inadequately formulated policy, in the worst case, will lead to a false sense of security.

Policy formulation ideally supports a thorough 'top-down' approach, in that it is an opportunity for top management to set a clear direction and demonstrate their support for and commitment to information security throughout the organisation.

An ideal security policy should provide guidance on the following areas (DTI 1997):

* The importance of information security to the business process

* A statement from top management supporting the goals and principle of information security

* Specific statements indicating minimum standards and compliance requirements for:

  - Legal, regulatory and contractual obligations

  - Security awareness and educational requirements

  - Virus prevention and detection

  - Business continuity planning

* Definitions of responsibilities and accountabilities for information security

* Details of the process for reporting suspected security incidents.

The contents of the policy should correspond and elaborate on the 'key controls' of BS7799, thus highlighting the importance and organisational wide implications of the policy. It is necessary to have a comprehensive understanding of information security and the policy, as this provides the foundation and environment for e-mail security. E-mail is an essential communications tool for organisations, both internally and externally, and thus must be recognised as an integral component to the overall information security strategy.

3. E-Mail Security: The Underlying Problem

'Computer networks are no longer defined by their physical boundaries; the communications revolution has delivered a powerful and indispensable business tool: E-mail.' Omniquad (1998)

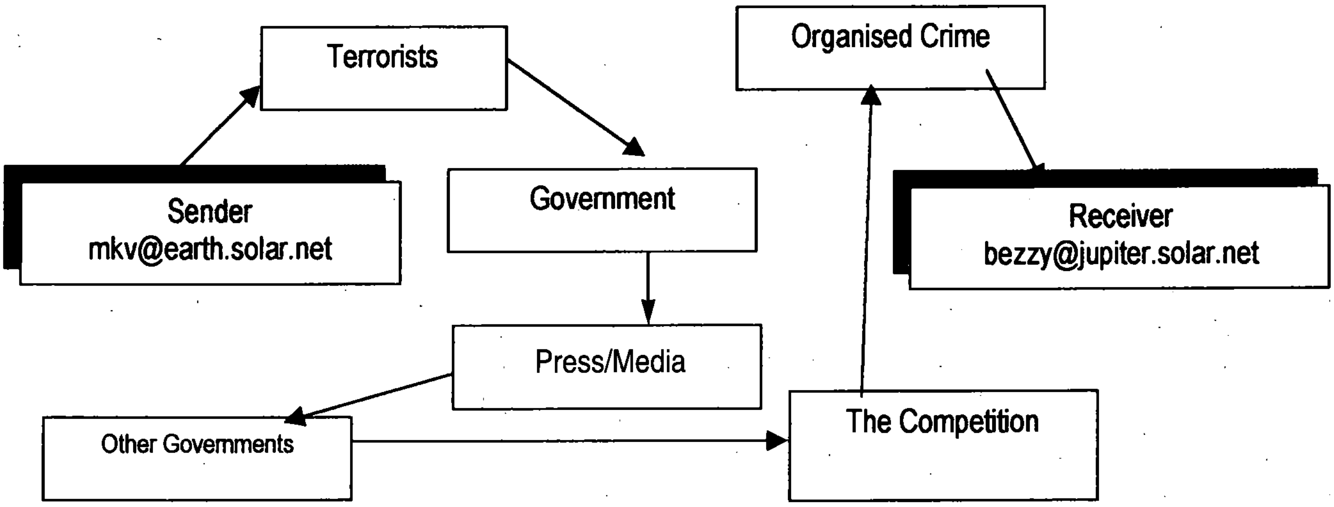
Although e-mail has increased the speed of communications and improved both organisational and business productivity; left unguarded or unprotected it is a potential threat to an organisation's integrity. It may also provide a damaging and accessible route for viruses, unauthorised access and overwhelming traffic loads; all of which can compromise the functioning of an organisation's network.

E-mail networks operate within decentralised networks, where an e-mail message is composed, using a MUA (Mail User Agent). However when an e-mail is sent, it is not sent as one whole message but it is broken up into various packets. A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network (WhatIs?.com). When an e-mail packet is sent from one place to another on the Internet, the TCP (Transmission Control Protocol) divides the file into 'chunks' of an efficient size for routing. Each of these packets is separately numbered and incorporates the IP (Internet Protocol) address of the destination. Individual packets from the same e-mail will travel across many different routes before arriving at the IP destination, where the packets are re-assembled into the original file.

It is the various routes that the packets employ that poses one of the largest threats to the integrity of e-mail. As the packets travel from their origin to their destination, they stop off at routers incorporated within various mail servers. The router is a device or a piece of software incorporated within a computer that determines the next network point to which a packet should be forwarded.

It is at this router that the e-mail packet is temporarily located and exposed, it is also possible at this point for a copy of the packet to be made at the router. During transit any intermediary based at one of the routers can quite easily read the packet unless it is encrypted or adequately secured. The intermediary could be anyone from a whole host of people e.g. the system administrator, a clever hacker or possibly even a regular user at the terminal. The intermediary can sit at the computer and see every e-mail that passes through the machine, no matter to whom it is addressed. The message can be printed or shown to other people, but much more significantly the message could be altered in transit.

The figure shows a hypothetical routing table that an e-mail packet could travel across prior to reaching its destination.



Routing Table

Table from Scheiner (1995; pp6)

3.1 The Invaders

Although a slightly exaggerated routing table, each of the intermediaries based at the routers all have a vested interest with passing e-mail packets. Each of these potential invaders will now be looked at as well as determining why each intermediary would be interested in e-mail packets.

4. E-Mail Threats

The main threats posed by e-mail will now be looked at. Once the threat has been established it will then be determined as to how a solution to the threat can either be provided or recommended.

4.1 Virus Infection

E-mail is one of the most popular channels for virus distribution, however there are many misconceptions in relation to e-mail and viruses, which will be clarified.

Fundamentally it must be acknowledged that it is not possible to receive a virus or any system damaging software by reading an e-mail; the e-mail being the actual message. A virus can not exist in an e-mail text message, viruses and other system-destroying bugs can only exist in executable files (.exe, .com), the only exception being if the text is written in HTML format within the mail, this will be executable.

Viruses are generally operating system specific, thus meaning a virus created for a DOS application can not damage a Macintosh computer. There is however one exception to the Operating System specific rule, this being a macro virus. One example of a macro virus is the Microsoft Word Macro Virus, which infects documents instead of the programmes. Macro viruses are computer viruses that use an application's own macro programming language to distribute themselves. As mentioned, a macro virus, will not affect the programme but instead will target the documents and templates.

Almost as disrupting as genuine viruses are hoax e-mails, warning of potentially dangerous viruses. Although hoax e-mails pose no danger to the system, they have certain negative implications on the user and the network. Primarily the network is affected as these hoax e-mails are usually forwarded messages and bulks of forwarded mail affects both network performance and consumes valuable bandwidth, Gerlitz (1999).

Hoax mail also affects the user. A well known hoax e-mail is the e-mail warning of the 'good times' virus, which even had governments concerned. The problem with hoaxes is that they usually request the recipient to forward the message to numerous people, thus redundantly wasting users' time and effectively consuming network resources.

Such hoax mail is sent to cause a nuisance, to irritate the user, to unnecessarily worry them and ultimately affect network performance. Hoax mail entails significant characteristics that distinguish it as being a hoax e.g. non-existence jargon, poor grammar and the absolutely ludicrous effects such as the A.I.D.S/Open virus[1]. It is up to the user to educate themselves and remain updated with e-mail hoaxes as well as genuinely damaging viruses such as the 'Melissa' virus[2].

Solutions for Protecting E-mails from Viruses

- Never download and/or run an attached file on an e-mail from a stranger or from an unknown address. Be very cautious when downloading/running files from friends; this is as if they pass you on a virus they will not know about it.
- Never have an e-mail programme set to automatically run attached files. This is especially true for browsers and/or e-mail programmes which automatically execute Microsoft word after opening an e-mail. Turn the option off to launch or execute any programs after receiving e-mail.
- Never run an executable file you've just received without first running it through an updated anti-virus utility.
- If the computer is on a network, it must be ensured that relevant security measures are in place to prevent unauthorised users placing files on either the computer or the network.
- The anti-virus software must constantly be updated by the vendor company.
- The e-mail programme must also be kept up-to-date. Security or loopholes are always being found with existing packages, a good vendor should post patches to update the package to any new threats.

4.2 Unauthorised Transfers and Offensive Content

This section will undertake an organisational perspective and will focus on organisations and their employees. E-mail has inadvertently allowed disillusioned or disgruntled employees to possess the ability to breach security and leak information at the click of a button.

There are many methods a disgruntled or soon to be laid off employee can use to damage his/her organisation. Primarily an employee could leak confidential information to rival organisations via e-mail, this task could quite easily be carried out undetected.

Also it would be an easy option for a sacked employee to unleash a virus they have been storing for such an occasion. This could be done directly from within the organisation or it can be carried out just as easily from outside the organisation by e-mailing an unsuspecting ex-colleague and requesting them to open an executable file containing a virus.

An unhappy employee could quite easily launch numerous e-mail bombs on the network. This task could be carried out in a variety of methods. They could set up the bomb using their own e-mail address or, more maliciously, another person's. The e-mail bomb is where a new or existing e-mail account is opened and literally bombed with hundreds of junk mail per day, possibly even an hour. When opening a new account or with an existing account, the e-mail address can be linked in with various additional information sites offering to post information on certain topics. This is potentially very damaging for both the organisation and the employee. Firstly, the employee user profile can either become corrupted or rendered useless due to the sheer volume of received e-mails. Secondly, the organisation's network can also be affected, as the incoming e-mails will be occupying a lot of the bandwidth, thus limiting resources and performance. If the volume of incoming mail exceeds the bandwidth, the network will slow down and ultimately may even crash.

Finally a disgruntled employee can damage an organisation by sending malicious or personally revealing e-mails about other members of staff, to colleagues and managers. This method can be done to greater effect if another employee's e-mail account or user profile is used.

[1] The A.I.D.S/Open Virus is a hoax mail warning of actual physical damage to the hardware

[2] The 'Melissa' virus is a typical macro virus, which has an unusual payload. When a user opens an infected document, the virus will attempt to e-mail a copy of this document to 50 other people using Microsoft Outlook.

Solutions for Unauthorised Transfers of Offensive Content

This aspect of e-mail security is where the security policy is so important. It is essential that in the policy there is a strict guideline and procedure for employees who have been sacked or laid off, and it is equally important to explicitly adhere to these procedures. The following recommendations can be incorporated into the security policy.

- As soon as an employee has received notification that their employment contract has been terminated, they should be escorted out of the building, under no circumstances should they be allowed to return to their terminals
- Make it company policy to actively promote security and ensure that all passwords are kept secure
- Ensure the mail server (or if in place, a firewall) checks all out going mail for leaked information
- Install the relevant anti-virus software
- Utilise firewalls in the distributed networks environment, to regulate incoming and outgoing mail
- Set up mail filters to block out bombs
- Ensure sensitive information such as redundancies or dismissals are always kept secret right up until the point of implementation.

4.3 Junk Mail (Spam)

Spam is the Internet's version of junk mail; an unsolicited, unwanted message sent to you without your permission (O'Reiley 1998; pp65-135). Most Spam messages on the Internet today are advertisements from individuals and the occasional small business. Spam messages are usually sent out using sophisticated techniques designed to mask the messages' true senders and points of origin. E-mail addresses are usually 'harvested' by Spammers from various sources such as web pages and downloading directories from the Internet Service Provider (ISP).

Spammers can argue that Spam is not a problem, that an unwanted message can easily be deleted, but Spam does pose a problem. Primarily Spam wastes the bandwidth of long-distance communications links and the time of network administrators who keep the internet working from day to day. Spam also wastes the time of countless computer users. Furthermore in order to deliver their messages, the people who send Spam messages are increasingly resorting to fraud and computer abuse. According to America On-Line, roughly a third of the e-mail messages AOL receives on any given day from the Internet is Spam.

Spamming could be seen as a form of advertising, but consider the cost implication; advertising in a newspaper costs anything between £5,000 to £25,000; sending out a catalogue to 100,000 people could cost anything between £75,000 to £175,000 depending on the print quality. A typical computer could connected to the internet over a 42 kbps dial-up modem can send more than 200 e-mails per minute, which translates into 1,728,000 messages a day or 52 million a month. With the on-going, government encouraged, price wars between ISPs a Spammer can roughly send 20,000 mail messages for a penny.

This low cost encourages Spammers to send huge numbers of messages, businesses that advertise using traditional media normally make some kind of effort to target their message to the relevant or appropriate market. However, Spammers have no motivation to target their messages because of the negligible costs of sending e-mails.

Solutions against Spamming

There are only two real countermeasures that can be undertaken against Spamming; filtering and replying back to the Spammers, or if the identity of the Spammer is known, they can be reported to the relevant authorities.

- Implement the appropriate filters incorporated within the designated e-mail package. All popular mail packages such as Macintosh, Euro Pro, Microsoft Outlook Express and Netscape Manager encompass extensive filtering methods, there are numerous strategies which a user can employ to block Spam.
- Respond to the junk mail; if it is possible to ascertain the Spammer's address, the Spammer's ISP could be alerted and notified of their behaviour. ISPs are usually very swift and clinical when dealing with Spammers.
- If the Spammer's address is obtained and known to be valid, the Spammer can be directly complained to.

5. Recommendations

5.1 Organisational Recommendations

RECOMMENDATION

1. Ensure the Overall Business Strategy Incorporates The Importance of Information Security

AIM

This proposal does not indicate that the business strategy should specifically include information security, but recommends that when formulating the policy the importance of information security should be appreciated. Also, by doing so, senior management can be made aware of the importance of information security.

IMPLEMENTATION

This can be achieved by the IT function stressing the importance of information security at top-level meetings.

Time: 3 -6 months.

Cost: No cost.

RECOMMENDATION

2. Compulsory Communication of Information Security Policy to all Employees

AIM

The aim of this proposal would be to make employees aware of information security, its existence and purpose within the organisation.

IMPLEMENTATION

A copy of the information security policy and its significance should be placed in the induction handbook, some reference should also be made to it when discussing the IT function.

Time: 4-5 weeks, the updating and re-printing of the induction handbook.

Cost: Dependent on the size of the organisation, and the printing size and quality of the induction handbook.

RECOMMENDATION

3. Incorporate E-mail Security into any Form of IT Training

AIM

To ensure that users are aware of the implications of e-mail security, and their own responsibility in the process.

IMPLEMENTATION

Any internal or in-house course that is operated by the organisation, pertinent to IT, should integrate the subject area of e-mail and its security. The user's role and responsibility in maintaining security should also be defined.

Time: 3-5 weeks, the revision and updating of current in-house courses.

Cost: No cost.

RECOMMENDATION

4. Increase Awareness of Commercially Available Packages

AIM

This would be applicable for senior management, it should be the responsibility of the IT department to keep up to date with the latest developments in security packages such as PGP and PEM. Newly introduced or updated packages on the market should be assessed, any productive and feasible implementations should be recommended to senior management. An ideal commercially available package should incorporate the following features:

- Confidentiality

- Nonrepudiation of Origin

- Data Origin Authentication

- Key Management

- Message Integrity

Protocols should also be considered; various users and networks use various protocols such as the SMTP protocol or the OSI communications framework. However protocols are now being designed with security as the primary consideration such as the S/MIME protocol.

IMPLEMENTATION

The IT department would have to closely monitor and assess the market for new developments in the security packages market.

Time: 4-6 weeks, this would be dependent on the product and the extent of the implementation. Updating a current package would take little time but communicating and training staff on either an updated package or a totally new package could take time.

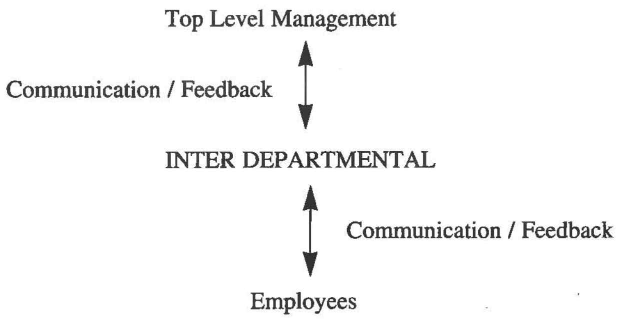
Cost: This again would depend on what product was being implemented, a single copy of PGP would cost approximately £40.00. However the training cost and implications, would be unaccountable.

RECOMMENDATION

5. Ensure Management Cascade E-mail Security Down to All Employees

AIM

This should be implemented so that e-mail security awareness travels top down within the organisation, originating from senior management through the relevant departments to employees within each department, as shown in the following diagram:



This diagram indicates that there is feedback, and it should be given at each level thus facilitating in the maintenance of general organisational awareness.

IMPLEMENTATION

There is no real direct or specific method that can be prescribed and adhered to, all senior management can do is ensure that they are actively participating in what is currently taking place and that all communication channels are open, specifically in relation to interdepartmental communication.

Time: This could take a very long time – anything to 6-12 months depending on an organisation's culture. If an organisation has an open communications culture, the basis would be there to develop interdepartmental communication and to increase the awareness and current proceedings in regards to e-mail.

Cost: There is no tangible cost that can be associated with this proposal.

RECOMMENDATION

6. Involvement of the Personnel Function

AIM

Within the organisational context it is very difficult to establish who is directly responsible for e-mail. Naturally the lab technicians or the systems support function are attributable to a certain extent, but they regard their responsibility as purely technical, in that they are only concerned with the maintenance of the network and its communication facilities. They take no responsibility in relation to the legal and organisational implications of e-mail, and often perceive themselves to be fragmented with the rest of the organisation, as they are not directly involved with the business goals or strategies. Therefore there must be a function that assumes responsibility – this is where the Personnel function can be incorporated. Legally there are four main reasons as to why the Personnel function would be concerned with the management of e-mail, these are:

* Use of e-mail for defamation, pornography and harassment

* Permanency of e-mail records and data protection legislation

- Accidental / Deliberate confidentiality breaches whilst using e-mail
- Distributing viruses.

By assuming allocated responsibility, the Personnel function can directly monitor and maintain some business implications of e-mail, thus devolving the responsibility from the systems support allowing them to concentrate on the technical maintenance of e-mail.

IMPLEMENTATION

The Personnel function could undertake the following measures and incorporate the following codes of practice:

- Advise staff e-mails are stored and can be read by the IT department
- Advise staff and managers of penalties for unacceptable use of e-mail
- Incorporate e-mail security into Disciplinary procedures and Equal Opportunities policies
- Incorporate into wider policies on 'secrecy' and data protection.

Employment contracts can also specifically deal with e-mail and cover copyright matters. Also e-mail can be used as tool for sexual harassment, thus possibly leading to the review of relevant policies, which therefore indicates that the Personnel have an important organisational role to fulfil within e-mail security. This could be indicative of the fact that rather than having one department or function solely responsible for e-mail and its security, such as the IT department or systems support, the responsibility of e-mail security should be devolved to separate functions.

The use of Personnel is also important when considering the growth of teleworking employees and their regulation, as e-mail is their primary communications tool. E-mail security could be integrated within strategic Human Resources Development plans through specific electronic and digital communications courses that could be offered in-house to employees.

Time: This would be an on-going process developing over time.

Cost: The developments would be internal thus cost would be minimal.

RECOMMENDATION

7. Set up a Steering Committee

AIM

A steering committee could be set up that has direct input from senior management and which organises regular interdepartmental meetings to discuss information systems security and monitor and review the organisation's current applications. Such meetings would ensure that an organisation develops its security thinking collectively. The steering committee could also monitor the external environment for developments and identify benchmarks or other organisations that can be seen to be operating 'best practice'.

IMPLEMENTATION

Ideally the committee should consist of current employees, who undertake the role within the committee as an additional task. Initially the committee should have a low key role within the organisation which can be developed depending on the success of the meetings and their outcomes.

Time: This would be an on-going process.

Cost: Internal recruitment would mean there are no extra costs.

RECOMMENDATION

8. Encourage Encryption in all E-mails / Keep Social E-mails to a Minimum

AIM

As highlighted in the survey, encryption was underused and social e-mails are quite significantly utilised; these proposals would facilitate the maintenance of the organisational network by not allowing it to become congested with unnecessary e-mails and would also protect the integrity by enchancing e-mail security through encryption.

IMPLEMENTATION

These are two fairly small proposals that could be communicated orally through department managers, via memo or notice boards.

Time and Cost: There would be no time and cost stipulations for these proposals.

5.2 Academic Recommendations

The academic recommendations are based on the information gathered and analysed throughout the paper, the actual proposals will be for the University of Greenwich.

RECOMMENDATION

1. Make IT Induction Compulsory for all New Students; within which E-mail Security is Covered

AIM

Many students believe that they had an inadequate induction to e-mail, the staff response is that a minimum number of students turned up at the optional induction. Therefore this induction should be made compulsory, during which e-mail security and the importance of user responsibility is outlined.

IMPLEMENTATION

This proposal could quite easily be implemented, as currently inductions are carried out and would just have to be updated to highlight the importance of e-mail security. However, the timing and structure of the induction would have to be revised to accommodate the large volume of students.

Time: This could be planned within 2 -3 months in preparation for the following academic year.

Cost: As there are already inductions in operation, there would be no extra cost.

RECOMMENDATION

2. Design a Leaflet Highlighting the Operation and Options Offered by the University E-mail Package

AIM

The leaflet should outline the basic functions of the package and how it operates. It should also incorporate e-mail security, its importance and the user's role, as well as the options available to the user. Rules and regulations in regard to e-mail should be explicitly defined, making clear what can and can not be sent.

IMPLEMENTATION

The leaflet should be designed by the lab technicians with user friendliness in mind, the leaflet should also indicate further reading or literature that would be useful if the student wishes to find out more.

Time: A leaflet could be drafted and produced within 3-4 weeks.

Cost: Cost would not have to be substantial, and printing costs could be absorbed internally.

RECOMMENDATION

3. Network Monitoring and Maintenance by Lab Technicians

AIM

The lab technicians should have clear set objectives about e-mail security and should work cohesively in actively promoting security-minded thinking. The University networks should be closely monitored and any common occurrences or regular inconsistencies, such as the congestion of undeleted e-mails, can be e-mailed to the user or placed upon notice boards around the University. Any new or updated information can also be distributed through these channels.

This would lead on to the technicians undertaking a more comprehensive responsibility for the security of e-mail. As established within the organisational context, responsibility can be devolved to various departments to increase the effectiveness of security. However, this is not possible within the University context, and the majority of the responsibility will have to be assumed by the technicians. Because there are various technicians at various sites, a clear set of objectives is required with clearly defined methods in attaining them. Lab technicians should provide a fairly fast network, which is not prone to congestion, however if this is unfeasible due to the physical limitations and bandwidth of the current network, recommendations should be passed to senior management requesting for funds to increase network capability and capacity.

IMPLEMENTATION

The implementation of this proposal would add to the technician's tasks but is essential if the users are to adapt a secure way of thinking.

Time: The only time implications would be on the technicians, who would have undertaken additional duties.

Cost: There would be no additional cost, except the additional hours taken on by the technicians.

RECOMMENDATION

4. Consider the Use of Commercially Available Software

AIM

Security is a rapidly developing area, and new additional 'transparent' software should be always be taken into consideration. Secure protocols, through which the user would not be disrupted, or perhaps security applications such as PGP could be set up within the profile and could be left to the user's discretion to utilise them, if and when required.

IMPLEMENTATION

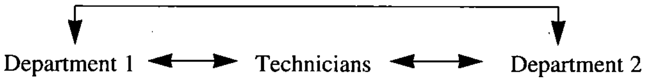
Implementation would be quite difficult, especially when updating the user profiles, as users would have to receive new information concerning the new applications.

Time: The process of actually placing the application onto the profiles ready for use would at the most take 2-3 days, however the real time implication becomes apparent when considering the training and education of users.

Cost: This would be entirely dependent on what product was being implemented, and the extent of its implementation.

RECOMMENDATION

4. Inter-Departmental Communication



AIM

As suggested in the organisational proposals, security should develop holistically at the same pace throughout the organisation. It is recommended that the same process should be attempted within the University context, however this can only be achieved through interdepartmental communication in which all departments ultimately report back to the technicians who are, idealistically, working together as a cohesive unit.

IMPLEMENTATION

Being an academic environment, the communication channels should naturally be fairly open. However it is the technician's role that is critical in this process. Their newly assumed responsibility will entail them obtaining information from the different departments and taking the relevant action.

Time and Cost: There are no time and cost stipulations.

7. Conclusions

The realistic aim of the recommendations, both organisationally and academically, is to effectively increase user awareness of e-mail security. However, as the recommendations indicate, e-mail security cannot be looked at abstractly, and there are many other encompassing factors. Idealistically if these recommendations are feasible and are effective they should promote a security way of thinking, rather than providing a rigid framework or structure.

Ultimately, information systems security and e-mail security should be 'transparent' in that there is no tangible structure to adhere to, security should be a way of thinking, which can only be brought about through awarcness. Frameworks and structures such as BS7799, security polices and codes of practice should be implemented to facilitate in the promotion of awareness. And it is the promotion of this awareness which should be targeted; organisations or relevant institutions should highlight the user's responsibility for ensuring their own security, through the aforementioned factors. However, this does not seem to be happening as innovations and developments are surpassing the emphasis for security implications, recent developments such as e-mail through digital television and e-mail on mobile phones such as the Ericsson T-28, highlight the fact that innovative thinking is being utilised rather than security thinking.

Bibliography

DTI (1997) - http://www.dti.gov.uk/SEC/

Gerlitz (1999) - http://www.gerlitz.com/virushoax/hoax2.html

Omniquad (1998) - http://Omniquad.com/

O'Reiley S and Schwartz (1998) - 'Stopping Spam', Cambridge Press.

Scheiner B. (1995) - 'E-mail Security, How To Keep Your E-mails Secure', John Wiley & Sons, pp3.

WhatIs?.Com (1999) - http://whatis.com/packet.htm

Mohammed Valji has recently completed his MSc in Distributed Computing Systems at the University of Greenwich. Mohammed's dissertation, on which this paper is based, researched the integrity and security problems concerning emails. He has extracted his main findings for this paper.

The Web Page

Copying from Cyerspace

Andrew Hawker
University of Birmingham

Plagiarism is flourishing, thanks to the Internet. In education, this is viewed with horror, as students can now download model answers and put together their essays using just a few *copy* and *paste* commands. For hard-pressed professionals, however, some of the materials available online can provide useful and legitimate short-cuts. Why draft your own report or policy document, for example, if someone has already been kind enough to put a suitable one on the Net?

There are a couple of American sites which are worth a visit from aspiring plagiarists. Both are run by agencies of the US Government. The Council of the Federal Government's Chief Information Officers has a site at **www.cio.gov**, and the General Accounting Office is to be found at **www.gao.gov**. The CIO site focuses very much on information technology, while the GAO investigates the use of public funds on behalf of Congress, and is more like the National Audit Office in this country.

Here are one or two suggestions for situations where computer auditors might find it useful to do a spot of plagiarism.

- Staff in your organisation are known to be using their office systems for all kinds of unofficial activities, and you have been asked to draw up some kind of policy document to deal with this. Where to begin? The CIO site offers an excellent blueprint, in the form of a document entitled: *Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" Of Government Office Equipment.* This can be downloaded as a seven-page Adobe document from **www.cio.gov/files/peruse.pdf**, and is one of a number of reports on security issues listed at **www.cio.gov/docs/Documents.htm#security**.

  The CIO guidance begins with some carefully worded definitions of basic terms such as "office equipment" and "employee non-work time". These are incorporated in equally well-crafted definitions of what is and is not to be regarded as permissible. The restrictions which are proposed are generally realistic - there is no attempt to ban every form of personal use. Of course, not everyone will have quite the same priorities as the US Government. For example, their employees are warned that if they engage in any private dealings with the outside world they must take care to avoid any impression of acting in an official capacity. Even in respect of internal communications, they are required to be "squeaky clean" in not giving any hint of bias or ridicule in sensitive areas such as sex, race and religion. Your organisation may need to extend or modify some of the provisions, particularly if it is outside the public sector, but the document provides an extremely useful place to start.

- You are under siege (yet again?) over questions of the cost-effectiveness of security measures. First port of call here is a short memorandum issued earlier this year on *Incorporating and Funding Security in Information Systems Investments*, at **www.cio.gov/docs/lews_lessons.htm** (memorandum M-00-07). This contains little which will surprise experienced computer auditors, but sets out general principles and justifications for spending on security in a clear and robust way. For more detailed ideas on implementing a security regime, the same site contains the *Federal Information Security Assessment Framework* (FISAF), as drafted this September, at **www.cio.gov/docs/information_security_assessment_frameworkv3.htm**. This defines five "levels of effectiveness" for a security programme. Again, some of the content is highly specific to the US government, but it provides straightforward and logical coverage of many of the key activities which are essential if an organisation's security is to be taken seriously.

For those who want an even more comprehensive review of security procedures and techniques the GAO offers a 276-page document entitled: *Federal Information System Controls Audit Manual.* FISCAM can be downloaded in Adobe format from **www.gao.gov**, and is to be found among the Special Publications on Computer and Information Technology, reference AIMD-12.19.6. A visit to the Table of Contents is obligatory before wading into the rather mixed bag of topics in this massive publication. Unfortunately the Adobe version seems to be entirely in image form, so that it is impossible to search by key word, and this also means that plagiarists will have a hard time lifting any of the useful passages. Nevertheless this is a useful source of reference on all kinds of issues. Journal readers may especially like to rate themselves against the *Knowledge, Skills and Abilities needed to perform Audit Procedures in a Computer-Based Environment*, as listed in Appendix V.

- Finally, it may be that you have been hit by a request to define policy on a more obscure area, such as whether or not cookies should be issued from the company's web site. **www.cio.gov** has a good search engine, with useful options to narrow the search (UK government sites, please note). This will lead you to a variety of documents, some setting out official policies, and others containing criticisms and comments. Cookie policy, in particular, appears to have stimulated some internal debate. See for example **www.cio.gov/docs/Cookiesresponse.htm**, where an earlier memorandum is taken to task for proposing a ban on all kinds of cookies, including those which could be short-lived.

Recalling the seasonal flavour which the Editor always brings to the December edition, I decided to challenge the CIO search engine with "Christmas" and "Tree". It found an occurrence of each, but not together. No joined-up government there, then.

Computer Fraud & Abuse Survey 2000

Chris Hurford

Associate Director, The Audit Commission

IT fraud and abuse is a headline-grabber and there is no shortage of tales of multi-million cyber crimes. But if management is to deal with the threat of computer misuse then it needs to be well informed about the nature of the risks that organisations face. But what is the truth behind all the stories?

The Audit Commission (the body responsible for the statutory external audit of local authorities and the NHS in England & Wales) began undertaking triennial surveys of IT fraud and abuse some 20 years ago to try and establish a better informed picture of the incidence of IT fraud and abuse in the public and private sectors of the UK.

The primary purpose of the Audit Commission's initiative has been to identify the nature of risks across all sectors and then to assess the likely impact on local government and the National Health Service in England & Wales. This provides valuable information for the Commission's auditors in helping their audited bodies to minimise risks of computer abuse and is equally useful to the wider audit and management community in the public and private sectors.

Key messages highlighted in the last survey included:

- a "control myopia" amongst management;
- the disappointing evidence of a continued absence of basic controls and safeguards;
- virus infections still accounting for the single most prevalent form of abuse - despite the widespread availability of both information on the subject and of safeguards;
- an almost three-fold increase in the number of incidents of hacking; and
- staff in managerial positions being responsible for 28% of frauds.

Overall, the picture which emerges from the last survey is one of little improvement in the safeguards adopted by organisations to withstand the threat of computer abuse with a disappointing catalogue of absent text-book controls, points to a continuing disregard for the basic tenets of security and safeguards. The most commonly cited reasons for fraud and abuse were a lack of management commitment, poor control over processing procedures and a lack of concern over preventing unauthorised access.

A little under a third of incidents were detected by internal controls and over half of all were discovered by accident. The importance of sound internal control mechanisms to prevent fraud and abuse cannot be over-emphasized and in the current climate of corporate governance and accountability, they have never been so firmly in the spotlight. The last survey seemed to indicate that for many organisations there was still work to be done.

The next survey invites participants to assess the risks to their organisations of IT fraud and abuse and invites them to describe any incidences they have suffered. We have defined IT fraud and abuse as including hacking, viruses, sabotage, theft of data and software, use of unlicensed software, misuse of personal data, inappropriate use of IT and unauthorised private work. Survey forms are being sent to heads of finance of 5000 public and private sector organisations and the report will be available in the early part of next year and a summary will be available on the Audit Commission's web site.

If your organisation has suffered from any form of computer fraud or abuse and you would like to contribute to the survey, please contact the CFS2000 unit in confidence at the Audit Commission, Nicholson House, Lime Kiln Close, Stoke Gifford, Bristol BS34 8SU on 0117 9236757 or fax 0117 900 1565 or email us at cfs2000@audit-commission.gov.uk

SETI at Home Update

John Mitchell

LHS Business Control

I am frequently asked how my involvement in the Search for Extra Terrestrial Intelligence (SETI) is coming along. To date I have processed 107 work units using a total CPU time of 5,360 hours. The totals for the project as a whole are provided below. As you can see, my contribution, using a couple of slow (266 & 300 Mega Hertz machines), is extremely small, but I am slightly exceeding the average work unit rate. For detailed information, visit www.setiathome.berkeley.edu.

As of yet, SETI@home has not detected any radio signals that indicate the presence of extraterrestrial intelligence. Thorough scientific analysis of the results returned by the SETI@home screensaver programmes is continuing. So far, SETI@home has received 233,238,007 results from all the SETI@home screensavers running around the world. This means that on the average SETI@home has received 92.85 results from each user.

Each result returned by the screensaver includes information about any significant spikes or gaussian signals detected in the analysis. The average result returned contained 4.95 significant spikes, for a total of 1,153,924,501 significant spikes detected by SETI@home users. The average result returned also contained 0.51 significant gaussian signals, for a total of 119,225,748 significant gaussians detected by SETI@home users.

With the release of the client screensaver version 3.0, SETI@home now looks for pulsed signals as well as triplets. Thus far, there have been 14,214,005 significant pulses and 16,534,848 significant triplets detected. Although SETI@home has not yet found any evidence of extraterrestrial intelligence, there are many signals that may prove to be extraterrestrial in origin once they have been carefully analyzed. The best 20 gaussian signals detected by SETI@home so far are available, ranked by their score. A map detailing the location in the sky of the best gaussian signals is also available. The results of some initial analysis of the spikes and gaussians are detailed in the science newsletters. Analysis of an interesting trend in the spikes is described in Science Newsletter #3. The initial SETI@home gaussian analysis is detailed in Science Newsletter #4.

QiCA: Being a Student: Getting Qualified, Getting Motivated

David Chadwick

University of Greenwich

In terms of gaining a professional qualification in computer auditing there are two main avenues open to a practising auditor: the Certificate in Information Systems Auditing (CISA) from ISACA and the Qualification in Computer Auditing (QiCA) from the IIA. The CISA and the QiCA approach the development of skills differently. CISA appears suited primarily to those who have already gained some working knowledge by virtue of having done the job for some time. The QiCA, however, is comprised of two papers at different levels; the lower level paper is perhaps more suited to the true novice, the practitioner with little experience or the student at university who both need to grasp fundamentals; the paper at the higher level is more appropriate for the experienced practitioner.

The professional bodies themselves provide distance learning courses or other arrangements for study but there are several universities around the UK who offer courses preparing students either to sit for the professional audit examinations directly or to gain exemption from the same by passing other recognised courses. City Business School, Guild Hall University, University of Central England, Southampton Institute, Sheffield Hallam University and University of Greenwich are but a few of those that provide courses leading to the two papers of the IIA's Qualification in Computer Auditing.

Three years ago, the School of Computing at the University of Greenwich applied to the IIA for recognition of existing undergraduate computing courses that covered auditing material at the lower level of the QiCA syllabus. The IIA responded by permitting students passing two particular courses at the university to apply for exemption from IIA studies at the lower level. This arrangement has been extremely beneficial for the teaching of computer auditing at the university.

Firstly, there has been a measurably greater interest in computer auditing throughout the student population during the past three years. The proportion of students choosing to do the optional audit-type courses has increased indicating a growing interest in wishing to learn about the subject. This has also been evidenced by the increased demand for audit-type books to be made available in the college library as well as access to journals and magazines.

Secondly, there are now several requests each year from students seeking audit-type jobs during their 'sandwich' third year of industrial training. Sadly, many have been disappointed as these types of jobs have not become available for students seeking their 12 month placement and many are forced to wait until graduation before seeking audit employment. But there has been a definite increase in final year undergraduates enquiring after auditing careers; throughout the spring months rarely a week passes without a student saying they have applied to one of the Big 5 or sought advice from the IIA regarding further study.

Lastly, and perhaps most interestingly, the average pass marks on the two qualifying courses have improved by almost 5% over the last two years. The university pass mark for a course is 40% but for IIA recognition students must achieve 50% in all coursework and all examination assessments. There is no doubt that the prospect of achieving recognition from a professional body is a motivating factor for the students; they undoubtedly work harder at assignments, turn up for lectures more frequently, and revise for examinations more thoroughly.

So what can we discover from all this ?

It does seem that computer auditing, as a career, is well served by being introduced to undergraduates at an early enough stage; at the very least it makes them aware that such a career is available. Also, it does appear that students are more motivated when their studies have some real-world goal particularly one that carries recognition from a professional body. Even those who profess no intention of taking up an audit career will openly say how much they now appreciate the need for controls and the role of the auditor in maintaining controls. And who knows - one day they may become the managers, the IT managers, the managing directors, the chief accountants, who need to stop occasionally and listen to what their auditors are saying.

DEAR EDITOR

According to the CCTA, security awareness is the most important and most difficult challenge in information security. I am seeking the views of information security, operational risk and audit professionals, as part of an MBA dissertation on human factors of information security.

Have you achieved management and staff commitment to information security? What techniques have you found particularly effective in embedding awareness and maximising co-operation across all levels of staff? Alternatively, what techniques don't work!

Would you be kind enough to call me any evening Monday to Saturday on 01202 604909. I will collate and share best practice gathered from the research with those who participate in a short informal interview.

I am relying on your help please, as a fellow practitioner and member of the security and audit groups.

Thank you,

Caroline Smith BSc MBCS CEng.

QiCA - The Qualification in Computer Auditing

The IIA-UK & Ireland has developed its specialist qualification in computer auditing to ensure that management can have access to auditors who have the necessary skills to give advice on achieving a balance between risk and control and on the key control implications arising from new technological developments.

About the qualification

The QiCA qualification comprises two levels, each with its own examination paper. The first level examination paper is *Information Systems Auditing* and the second level paper is *Specialist Information Systems Auditing*. Students enrolling on the QiCA qualification must take a formal course of study leading to the first level examination Information Systems Auditing. There are a number of approved tuition providers in the UK offering courses of study for this paper and the IIA-UK & Ireland also runs its own Distance Learning course.

SYLLABUS CONTENT

Information Systems Auditing

This paper has been designed test your general understanding of the principles and practices of information systems auditing. The topics you will study include:

* Control in information technology systems
* Information systems strategy and development
* Information systems security operations
* Software
* Basic CAATs
* Control and audit applications
* Communications and networks
* End-user computing
* Computcr misusc and thc law

Specialist Information Systems Auditing

This paper is focuses on some of the more technical issues and is aimed at those who carry out 'hands-on' computer audits of a technical nature.

There are five specialist areas:

* IT Management
* Systems Software
* Security & Contingency Planning
* Networks and On -Line Systems
* Auditing Applications and Advanced Systems

QiCA - PRACTICAL EXPERIENCE

Practical experience is an integral part of the qualification and you will be required to maintain a log of your practical work. A logbook will be sent to you when you enrol as a student. Having passed the examinations you will be required to provide evidence that you have achieved 1600 hours computer auditing related work experience over a period of at least two years.

On approval of your logbook you will be awarded the QiCA qualification, admitted as a member of the IIA-UK & Ireland and be entitled to use the designatory letters, QiCA.

SAP R/3 v.4.6 New Functionality

Bob Ashton

Queensland Audit Office

SAP has announced that maintenance for version 3.x is to be discontinued in 2001. A brief overview of new and amended security and user functionality for version 4.6 follows:

New Functionality

1. User Role Templates
The new version includes over 100 new user role templates.

2. Flexible User Menus
SAP Standard Menu:
User menus will now only display the options which the user has been granted.
A user can create a personal favourite list of transactions.

3. Composite Activity Group
It is now possible to create a Composite Activity Group, which contains a collection of other Activity Groups. Composite Activity Groups contain only Activity Groups and no authorisation data.

4. Central User Administration (CUA)
User data can be maintained centrally for all systems and clients, or distributed.
Flexibility has been introduced to allow sections of user data to be maintained centrally and/or locally. The Global User Manager tool with drag and drop interface for users, user groups, systems and activity groups is an important innovation.

5. User Groups
User Groups are now used for better distribution of user data, increasing the use of CUA. SAP has extended the User Group feature to create a link to Activity Groups.

6. Mass User Maintenance
The Mass User Administration function has been extended to include mass changes for login data, default values, parameters, activity groups and profiles.

7. User Interface
The upgrade involves major changes to the user interface.

Changes to Existing Functionality

1. Profile Generator Changes
Reports, Transaction Variants - web addresses and activities can be added to an Activity Group. Using the Profile Generator the menu nodes a user will see on login can be moved and renamed.

2. CCMS Security Audit Logs and Alerts
A new monitoring object - "security", has been introduced for the display of security status information. Security-related system events are now also visible from within the Computing Centre Management System (CCMS). For each security-related event that is captured by the active Security Audit Log configuration, an alert can be passed on to the CCMS.

3. Changes to SAP Transaction Codes
As part of the changes to the menu system, SAP has also changed the look, processing logic and codes of some transactions. The most commonly used transaction codes (approx. 25 in total) have been changed. The new version supports approx. 56,000 transactions, compared to approx. 12,000 in 3.1.

4. Reports
SAP has indicated that all reports have been linked to a Transaction Code.
These reports can be assigned to an Activity Group by either assigning the new Transaction Code directly or by searching a Report Tree and selecting the report.

5. HR Security
HR position based security has changed to be more activity group focused. This supercedes the use of the 1016 infotype and the RHPROFLO program.

6. Changes to Tables
Important security tables no longer exist and have been replaced by new tables. Major changes have been made to user tables.

As can be seen, the introduction of version 4.6 is likely to have major implications for auditors of SAP R/3 in the coming year.

BCS MATTERS!

Colin Thompson
BCS Deputy Chief Executive

Colin Thompson, BCS Deputy Chief Executive, reviews some of the current BCS news items. Further information on these or any other BCS related issues may be found on the BCS Web site ("http://www.bcs.org.uk/")

Information is also available from Customer Services at The British Computer Society, 1 Sanford St, Swindon SN1 1HJ (e-mail to marketing@hq.bcs.org.uk)

New Faces at the top

The Annual General Meeting, held at Church House Westminster in October, saw the hand-over of the presidential baton from David Hartley to Alastair Macdonald. Until his retirement earlier this year, Alastair was Director General of the Industry Group at DTI, a job that brought him into a close association with the IT and electronics industries. His responsibilities included the DTI's Communications and Information Industries Directorate and the Radiocommunications Agency (where he chaired the Steering Board).

Alastair has long been involved with the IT industry: he was the Under Secretary in charge of the IT division during IT Year 82, a member of the Alvey Committee, and the Under Secretary in charge of the DTI's Telecommunications division when British Telecom was floated in 1984.

The AGM also marked the election of a new Deputy President, Geoff McMullen and two new Vice Presidents. Geoff has enjoyed 37 years working in IT and is currently the Chief Executive of Ukerna, the agency responsible for the Joint Academic Network (JANET). His earlier career included jobs with NCR, Babcock & Wilcox, CEIR, UNIVAC and Shell.

The two new Vice Presidents are John Chapman, who succeeds Geoff McMullen as VP Professional Formation, and John McDermid who takes on the role of VP Engineering.

AGM Lecture

The formal business of the AGM was followed with a lecture given by Jim Norton. Jim is the Head of E-Business Policy at the Institute of Directors and was formerly the Director of the Cabinet Office Performance & Innovation Unit (PIU) e-commerce team. In his lecture he described how the new tools of e-business will have a fundamental impact on companies, large and. small, in both the old and new economies. He gave practical examples of how these tools are exploited today to transform the business model of many organisations, and examined how companies can combine the best expertise of conventional business with the new tools of e-business. This was illustrated with examples of successful e-business developments from both the UK and USA. Jim also reflected on the progress made one year on from the publication of the PIU report to the Prime Minister - "e-commerce@its.best.uk"

The PowerPoint slides used to illustrate the lecture are available for download from the BCS Web site (http://www.bcs.org.uk/news/2000/agmlec.htm) - but be warned, this is a large file that will take some time to download.

And some departures....

Sadly, the last few months has also seen the departure of two long serving and distinguished members, Ron McQuaker and Donald Davies.

Ron was BCS President for 1996-97, and an active member for many years, serving on the Council as an elected member, as Vice-President (Professional) from 1991-94, and as Deputy President in 1995-96. He chaired the Intellectual Property Committee and the joint BCS/IEE Working Party on Competencies, Education and Training. He was founder and chair of the Legal Affairs Committee in 1998.

Donald, who died on 28th May at the age of 75 was a Distinguished Fellow of the Society and will be remembered as the pioneer of packet-switching and for his work on security, particularly in the area of public key encryption.

Such was Donald's eminence that the BCS and the IEE arranged a memorial lecture in his honour. At that event, in early November, three speakers paid tribute to his achievements - Roger Scantlebury, Professor Henry Beker and Dr Vinton G Sert.

BCS Awards

The BCS runs two major award schemes each year - the IT awards, for excellence in computing which reach their conclusion each autumn and the IT Management Awards, for excellence in information systems management, which are decided in late spring.

60 applications were received for this year IT awards and medals were awarded to 7 projects. Three equal winners, chosen from the medallists, received their awards from the Duke of Kent, the Patron of the BCS, at a dinner held in London on 1st November:

The *Digital Audio Broadcast System* from RadioScape Ltd is a software based system for the transmission of digital radio, requiring only an industry standard PC, running Windows NT. This significantly reduces the cost of digital radio transmissions to broadcasters. The software defined radio technology will also drive down the cost of digital receivers, making digital radios more affordable to the UK public.

Arjuna Software, the second winning project, was developed by the Distributed Systems Research Group led by Prof Santosh Shrivastava of the Department of Computing Science of The University of Newcastle. The Group has spent several years researching the development of concepts and techniques for building robust distributed systems and has contributed to the development of a number of industry standards on open distributed computing as well as creating products for enabling Internet based transactions.

The third award went to a consortium comprising the Post, TeleVirtual and the School of Information Systems at the University of East Anglia Office for *TESSA (Text and Sign Support Assistant)*. TESSA allows speech to be transformed into sign language for the benefit of deaf customers in Post Office locations and is leading the way internationally in improving levels of service for deaf people.

Towards a More Secure World

News of moves to improve the service which the Society provides in the area of information systems security. The main driving force behind these moves has been Rodney Clark, chairman of the Information Security Specialist Group, working with staff in BCS headquarters and with other BCS groups in the security and privacy field. The aim of the work is to improve the quality of the information provided and to present a more coherent picture of the various strands of BCS security related activity.

The first visible result of this work was a 4-page brochure describing the full range of BCS security related services and activities. The brochure was published in April in time for the InfoSecurity show and copies are available from the marketing Department at BCS Headquarters. More recently, on 16 November, a group of around 25 people gathered for an evening meeting in the London HQ building to discuss ways in which this work can be taken further. That debate will be continued by e-mail and through a dedicated bulletin board. Comments from members of the Audit Specialist Group are welcome - ideally by e-mail to me (cthompson@bcs.org.uk).

BCS Branding

BCS branding is currently under the spotlight as a result of a project designed to clarify the BCS image and to ensure that it is projected more consistently through a well managed strategy. The project is being directed by Charles Hughes, one-time senior manager within ICL, supported by Clark Hooper Momentum, a London-based agency specialising in branding work. The project is scheduled for completion in early February and the deliverables will include a new logo together with a strategy for managing the brand across all areas of the Society.

As with all brand management, one of the most important tasks will be to ensure that the experience of members and customers in using the BCS services is consistent with the image we project through our branding strategy - in other words, that our brand values reflect reality rather than wishful thinking.

Although the branding project is moving at a fairly fast pace, we are trying to ensure that all parts of the BCS are kept informed and consulted. Focus group sessions are being held for both branch and Specialist group representatives and the agency briefing document, which forms the basis for the project, is available for download from http://www.bcs.org.uk/temp/brand0910/brief.htm

Programme 2000Plus - The BCS Change Programme

The Branding Strategy is just one of a number of change projects that fall within the umbrella of Programme 2000Plus - of which I have written much in previous editions of this newsletter. Other elements include the project to extend and improve our Web site, the extension of the grading structure as recommended in the Pollard report of 1998 and the introduction of a new organisational structure. Overall, the programme is intended to transform the BCS into a modern professional body, with a clearly recognised position of leadership within the IS community, respected by practitioners, employers, government and the wider public for the quality and value of the services provided.

Whist much of the detail relating to the necessary changes has yet to be worked out, the essential foundations are clear:

* A much closer understanding of the needs, aspirations and perceptions of our constituency as the basis for all that we do;

* Clear statements of corporate direction, including medium and long term objectives, as the basis for all our business planning;

* Customer focused service delivery, to meet those objectives, with all services available through a modern, well designed web-based interface;

* Professional marketing and communications support to ensure a consistent message both internally and externally;

* An organisational structure designed to mobilise and focus all available resources - including particularly the experience of our members, and the efforts of branches and specialist groups.

It will be no small task to build and maintain the required capability within BCS. However, the recognition of the need to make the changes was very clearly evident amongst members of the Policy and Resources Committee when the issue was discussed at their annual Away Weekend in September.

The full programme to transform the BCS will take several years to complete but the new branding strategy and initiatives such as that in the security area described above, will be important steps along the way.

A New Organisational structure

The structure of the member organisation is an important element of Programme 2000 Plus - and one that received particular attention at the Away Weekend. Organisational structures must of course be considered in relation to purpose and, for BCS, the essential need now is to harness resources more effectively and to improve the focus on service delivery and corporate objectives. Against that background, the PRC is exploring, subject to Council approval and to consultation with members, a structure based on four Boards, in place of the existing seven, plus three Fora, each led by a Vice-President.

Under these arrangements it is the intention that Boards should be responsible for delivering the programmes of the Society and that they should be sized appropriately for the task, including only those necessary to conduct the work. Representational membership of Boards would not be a pre-requisite and as far as possible work would be taken forward by task based groups with a limited lifespan, rather than by standing committees. Working titles for the proposed four Boards are:

* Member Services

* Qualification and Standards

* External

* Dissemination of Knowledge

BCS MATTERS!

Under these arrangements the responsibility for both Branches and Specialist Groups would fall to the new member Services Board. This Board would have would have overall responsibility for ensuring that the Society is providing its members with the information and related services necessary for effective professional practice at all levels.

Fora are intended to be much looser organisations pursuing matters of interest to a common community. The ideas would be expected to arise mainly from bottom up, and activities will be focused on participation and networking. The Fora under consideration are those identified as potential colleges in the work of Programme 2000 Plus. They are:

* Engineering

* Management

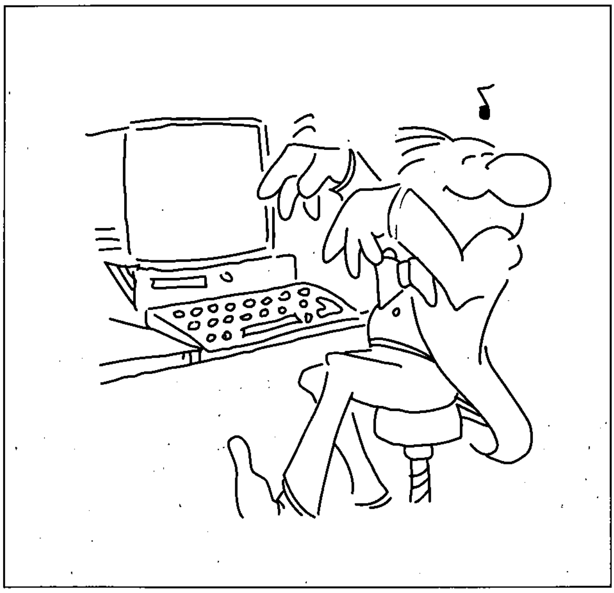
* Education

And Finally........................

My very best wishes to everyone for Christmas and the New Year.

Caption Competition

The best caption to the cartoon below, received by 14th February 2001, will receive a gift voucher. Suggestions to the Editor at the email address on page 3.



HUMOUR PAGE

Exam Questions & Answers

Once again I draw on various sources to help enlighten your seasonal quizzes (Ed)

Q: Name the four seasons.
A: Salt, pepper, mustard and vinegar.

Q: Explain one of the processes by which water can be made safe to drink.
A: Flirtation makes water safe to drink because it removes large pollutants like grit, sand, dead sheep and canoeists.

Q: How is dew formed?
A: The sun shines down on the leaves and makes them perspire.

Q: What is a planet?
A: A body of earth surrounded by sky.

Q: What causes the tides in the oceans?
A: The tides are a fight between the Earth and the Moon. All water tends to flow towards the moon, because there is no water on the moon, and nature abhors a vacuum. I forget where the sun joins this fight.

Q: What guarantees may a mortgage company insist on?
A: If you are buying a house, they will insist you are well endowed.

Q: In a democratic society, how important are elections?
A: Very important. Sex can only happen when a male gets an election.

Q: What are steroids?
A: Things for keeping carpets still on the stairs.

Q: What happens to your body as you age?
A: When you get old, so do your bowels and you get intercontinental.

Q: What happens to a boy when he reaches puberty?
A: He says goodbye to his boyhood and looks forward to his adultery.

Q: Name a major disease associated with cigarettes.
A: Premature death.

Q: What is artificial insemination?
A: When the farmer does it to the bull instead of the cow.

Q: How can you delay milk turning sour?
A: Keep it in the cow.

Q: How are the main parts of the body categorised? (e.g. abdomen.)
A: The body is consisted into three parts - the brainium, the borax and the abdominal cavity. The branium contains the brain, the borax contains heart and lungs, and the abdominal cavity contains the five bowels, A, E, I, O and U.

Q: What is the Fibula?
A: A small lie.

Q: What does 'varicose' mean?
A: Nearby.

Q: What is the most common form of birth control?
A: Most people prevent contraception by wearing a condominium.

Q: Give the meaning of the term 'Caesarean Section'
A: The caesarean section is a district in Rome.

Q: What is a seizure?
A: A Roman emperor.

Q: What is a terminal illness?
A: When you are sick at the airport

Q: Give an example of a fungus. What is a characteristic feature?
A: Mushrooms. They always grow in damp places and so they look like umbrellas.

Q: What does the word 'benign' mean?
A: Benign is what you will be after you be eight.

Q: What is a turbine?
A: Something an Arab wears on his head.

Queensland Comptruckr Terms

TLA's are hard enough to deal with at the best of times, but our antipodean cousins go one better by completely redefining every day computing terms. Try these after a few seasonal drinks (Ed).

1. Log on: Make the barbie hotter
2. Log off: Don't add any more wood
3. Monitor: Keep an eye on that barbie
4. Download: Getting the firewood off the truck
5. Floppy disk: What you get from trying to carry too much firewood
6. Ram: Kiwi's brother-in-law
7. Hard drive: Getting home in a heavy rain storm
8. Prompt: What the postal service used to be
9. Window: What to shut when it's cold outside
10. Screen: What to shut in mosquito season
11. Byte: What mosquitoes do
12. Bit: What mosquitoes did
13. Mega Byte: What Townsville mosquitoes do
14. Chip: bar snack
15. Micro chip: What's left in the bag after you eat the chips
16. Modem: What you did to the hay fields
17. Dot matrix: Old Dan Matrix's wife
18. Laptop: Where the car sleeps
19. Software: The plastic knives and forks they give you at Red Rooster
20. Hardware: The real stainless steel cutlery
21. Mouse: What eats the grain in the shed
22. Mainframe: What holds the shed up
23. Enter: City talk for "it's open"
24. Web: What a spider makes
25. Website: The shed, or under the verandah
26. Cursor: Someone who swears
27. Search Engine: What you do when the truck won't go
28. Screen Saver: Chicken wire
29. Home page: Parawunda phone book
30. Upgrade: Steep hill
31. Server: The person in the hotel who brings the counter lunch
32. Mail Server: The bloke at the hotel who brings the counter lunch
33. Sound Card: The one that wins the hand of 500
34. User: The neighbour who keeps borrowing stuff
35. Network: When you have to repair the fishing net
36. Internet: Complicated fish net repair method
37. Netscape: When a fish manoeuvres out of reach
38. Online: When you get the laundry hung out on the wash line
39. Offline: When the clothes pegs let go and the laundry falls on the ground

Notes:
Truck: Australian for pick up truck. An abbreviation of utility vehicle

casg
Computer Audit
Specialist Group

British
Computer
Society

Registered Charity No. 292786

PLEASE RETURN TO

Janet Cardell-Williams
CASG Administrator
49 Grangewood
Potters Bar
Herts EN6 1SL
Fax: 01707 646275

Membership Application

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

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

CORPORATE MEMBERSHIP (Up to 5 members) * £75

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

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

INDIVIDUAL MEMBERSHIP *(A members of the BCS)* £15
BCS membership number: ______________________

STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment).
Educational Establishment: ______________________________ £10

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE:
(STD Code/Number/Extension)

E-mail:

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)

E-mail:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

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

casg
Computer Audit Specialist Group

British
Computer
Society

Registered Charity No. 292786

Management Committee

CHAIRMAN	John Bevan	Audit & Computer Security Services	01992 582439 john.bevan@virgin.net
SECRETARY	Raghu Iyer	KPMG	020 7311 6023 raghu.iyer@kpmg.co.uk
TREASURER	Mike Demetriou	CrestCo Ltd	020 7849 0000 mike.demetriou@crestco.co.uk
MEMBERSHIP SECRETARY	Jenny Broadbent	Centrica plc	01784 645688 jenny.broadbent@centrica.co.uk
JOURNAL EDITOR	John Mitchell	LHS Business Control	01707 851454 john@lhscontrol.com
WEB MASTER	Siobhan Tracey	Booker plc	01494 442883 siobhan.tracey@bbw.booker.com
SECURITY COMMITTEE LIAISON	John Bevan	Audit & Computer Security Services	01992 582439 john.bevan@virgin.net
TECHNICAL BOARD LIAISON	Vacant		
TECHNICAL BRIEFINGS	Paul Plane	Dai-Ichi Kangyo Bank	020 7283 0929 x 1222 pplane@dkbeurope.com
MARKETING	Steve Pooley	Independent Consultant	01580 891036 steve.pooley@cast.com
ACADEMIC RELATIONS	David Chadwick	Greenwich University	020 8331 8509 d.r.chadwick@greenwich.ac.uk

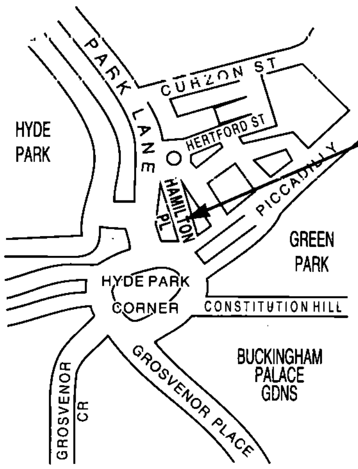
Membership Enquiries to:

Janet Cardell-Williams
49 Grangewood
Potters Bar
Herts
EN6 1SL

Fax: 01707 646275
Email: members.casg@bcs.org.uk

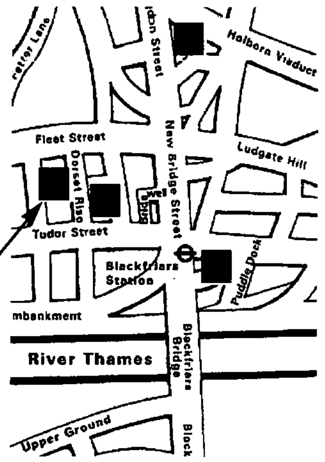
Venue for
Full Day Technical Briefings

Venue for
Late Afternoon Meetings



Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ

KPMG
8 Salisbury Square
London EC4



GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

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

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

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

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

ADVERTISING IN THE JOURNAL

Reach the top professionals in the field of EDP Audit, Control and Security by advertising in the CASG Journal. Our advertising policy allows advertising for any security and control related products, service or jobs.

For more information, phone John Mitchell on 01707 851454.