ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 9 NUMBER 4 AUTUMN 1999

The British Computer Society

Proposed programme for the 1999/2000 season of members' meetings

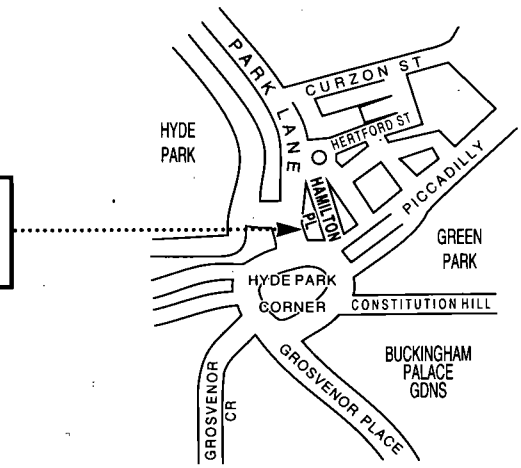
September 28th 1999	Year 2000 contingency planning	Late afternoon
November 9th 1999	Why risk IT? (to include control risk self assessment, risk based audit planning, etc.)	Full day briefing
December 7th 1999	Data Protection Act	Late afternoon
January 25th 2000	Basic Internet security, to include e-mail and Web surfing risks and controls	Full day briefing
April 4th 2000	E-commerce security, going beyond basic Internet risks covered in the earlier meeting	Full day briefing
May 16th 2000	BS 7799 developments	Late afternoon

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.

Final arrangements are still being made, so dates may change. For final details, from early September please refer to the Specialist Groups section, CASG meetings sub-section, of the BCS Web site at http://www.bcs.org.uk. There you will find CASG administrator's and committee members' names, phone numbers, and other contact details. Members will receive full details when these have been finalised.

Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ



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 PostScript, Berkhamsted, Herts.

EDITORIAL

Ever since the Norwich Union was fined as a result of one of its employees making derogatory remarks about a competitor on Norwich's own, internal email system, I have been wary about the amount of information that companies hold on their employees' working habits in the form of archived email messages. Indeed, I have had occasion to use the archived material myself when conducting special investigations and have been amazed by the wealth of information at my disposal. Not so much on the content, but the revelations of the different working styles of each employee. Their times of attendance can be gauged from the time stamp of their first and last email of the day, their absences from work, those who work at weekend. In many cases, their response speed and productivity can be determined. Why use time and motion studies, when much of the information required is being quietly gathered by the company file server on a minute by minute basis? Which brings me to this edition's major article, which is on the subject of email policy setting. The author, Sally Burfoot, made this her dissertation subject for her MBA at the University of Surrey. Not many organisations start at the top by designing an appropriate policy which is then supported by standards and procedures. Most start at the bottom and are eventually forced to work their way upwards. Here is your opportunity to do it the right way.

We also have a report from Mike Demetriou, our Treasurer, on the Group's financial position and the usual column from Colin Thompson reporting on the activities of our parent organisation. It is nice to see that William List, a previous Chairman of this Group has received an honoury Fellowship. A very deserving award for someone who Chaired this Group for seven years and then went on Chair the BCS's prestigious Security Committee. I also notice that Colin himself is now Deputy Chief Executive of the BCS. Well done Colin and please keep your column coming.

In conclusion, David Chadwick of Greenwich University makes an impassioned plea for work experience for his students. Take his examination and see how your company measures up.

Happy reading.

John Mitchell

Chairman's Corner

John Bevan

One of the things that distinguishes a good sports club from others is the time and effort spent both on finding new members and on encouraging those new to the sport. Without this a club may just fade away as its members get older. With a special low subscription rate CASG has always encouraged students to join. The management committee discussed "students" at a recent meeting, and decided it wanted to do more for them. We agreed on two immediate actions: to offer genuine, full time students admission to any full day Technical Briefing in the 1999/2000 programme at the much reduced rate of £25, and to ask David Chadwick, a lecturer at Greenwich University, to join the committee with a special brief to develop our approach to student matters and to act as our link with others teaching computer auditing. Whilst this is a good beginning, we want to explore and develop other ideas, listening carefully to feedback.

David and I would welcome experienced computer auditors who could talk to students, at a college venue, and on a voluntary basis, on what it is really like working as a computer auditor. If you might like to do this, then please contact David or me. We are open to other ideas, such as help with industrial placements, special meetings, or giving space at meetings or in our Journal to research projects and theses.

You can contact David Chadwick at Greenwich University, by e-mail to D.R.Chadwick@greenwich.ac.uk.

I am sure that you will be able to read more about him in a future issue of the Journal.

Alternatively, and out of term time, contact me.

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, Ami-Pro, or ASCII format. Electronic submission is preferred.

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

Submission Deadlines

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

Developing a Framework for the Design and Implementation of an E-mail Policy Within a Large Organisation

Sally Burfoot

1. Introduction

In the broadest sense Electronic mail (E-mail) refers to any electronic alternative to the traditional paper-based postal service. This includes 'facsimile, telex, communicating text processors, message-switched networks and computer-based messaging systems' (Zorkoczy, 1990, pp.127). For the purposes of this article the emphasis is on the latter.

The traditional E-mail system has many different capabilities making it an important organisational communication tool. The business benefits of a E-mail system are that it eliminates telephone 'tag'[1], is less costly and provides more flexible systems which expedites communication within an organisation. Newer systems such as Lotus Notes[2] also offer a fully integrated 'workflow' application and have the potential to increase a company's competitive advantage

Although, the concept of E-mail is similar to the traditional paper-based mail system its use raises a number of managerial issues which are generic to the use of IT and not necessarily encountered with a traditional mail system. These issues include the fact that it can only be used by individuals who can, or are willing to type and have access to the necessary equipment, the privacy and security of the communication, an individual's right to free speech, the ability of data to cross national and international boundaries, the ethics of using or implementing IT as well as which technology to use and the justification of its purchase.

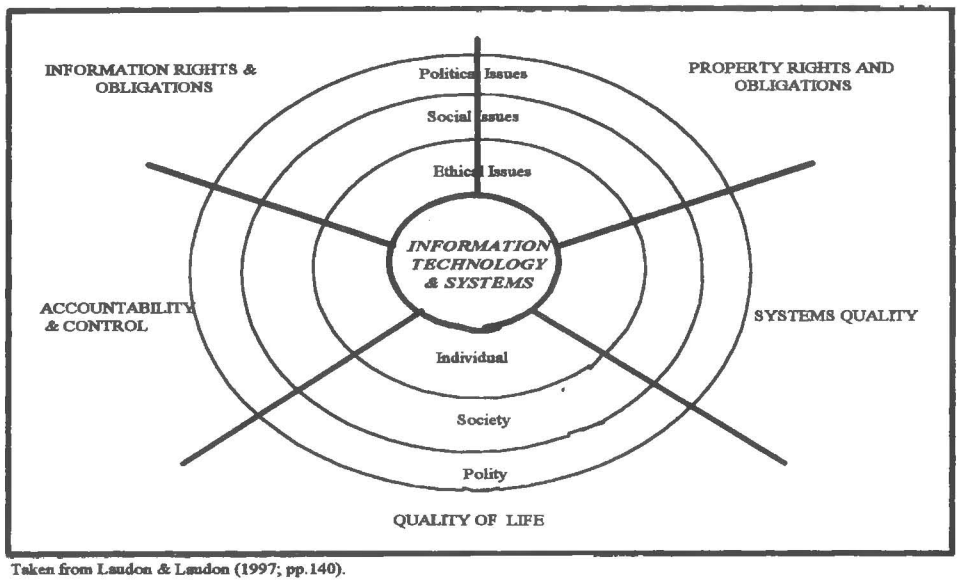
The nature of these issues means they are inextricably linked and need to be fully understood before a company can develop and implement a policy relating to the use of E-mail. One model proposed by Laudon & Laudon, (1997) and illustrated in **Figure 1**, attempts to explain the impact of technology and more specifically the relationships between the different issues by using the analogy of 'throwing a stone in a pond'.

The various issues, or moral dimensions associated with the use of technology can be viewed as sitting in a pond, rather like lillies and technological innovations or 'events' represented by a stone. Every time a stone is thrown into the water it causes a rippling effect in all directions cutting across all issues at every level - individual, social and political.

The fact that every issue associated with the use of E-mail impacts upon and is itself affected by other issues makes designing a policy complicated. The difficulty lies in defining the boundaries between the different issues. For example, where does freedom of speech end and an individual's right to privacy begin?

Although, the formulation of a policy may be difficult, according to the Commission on Social Justice, policies are essential in order to protect the individual. The pressure for controlling the use of E-mail is intensifying as what began as a 'add-on' facility to desktop applications is now being used so extensively that increasing proportions of a company's IT budget is needed to support and sustain the system.

The aim of any policy therefore, is to enable the benefits such as efficient communication to be utilised while at the same time protecting the rights of employees, the company's integrity and its information assets.



Taken from Laudon & Laudon (1997; pp.140).

Figure 1 - A Model of the Ethical, Social & Political Issues Facing IT Managers

[1] Repeatedly leaving messages for and missing calls from an individual.
[2] A computer-based messaging system developed by Lotus Corporation

2. Research Findings

The aim of the literature review was to gain an understanding of the managerial issues associated with the use of E-mail. These issues included; legislation, freedom of speech, privacy, ethics, security and justification of the investment in technology.

Currently, the only traceable English law relating directly to the use of computers is the Computer Misuse Act 1990 which makes unauthorised access to computer material, unauthorised access with intent to commit or facilitate the commission of further offences and the unauthorised modification of computer material, a criminal offence.

Despite this apparent lack of legislation there are other legal considerations to be taken into account. Namely; the Companies Act 1985, Civil Evidence Act 1995, Data Protection Act 1984 (and 1998) and the Interception of Communication Act 1985 - details of which are summarised in **Table 1**.

In terms of liability, in England 'wherever an employee uses E-mail in a way that is contrary to statute or infringes the rights of others, the employer may find itself liable for the employee's conduct' (McGrigor Donald, 1996; pp.1). Liability also extends to the loss of revenue or damages incurred by an individual or an organisation in the event of a virus being transmitted via the E-mail system and to the infringement of copyright laws. Both here and in America, copyright protects an individual's property right by verifying that permission is needed from the originator before the information can be used (Thomas *et al.*, 1998).

In America, which appears to be more advanced in terms of addressing legislative issues than the UK, the courts have equated an E-mail system within an organisation to a book shop. Meaning, the owner could not be expected to read all the books on sale. As such, if a company claimed not to screen the messages sent via E-mail then they could not be held liable for their content unless it was proved otherwise (Ackerman, 1995).

Two other issues relating to the use of E-mail and which are directly affected by legislation are freedom of speech and privacy. Both of which warrant further discussion.

Although, the right to freedom of speech is contained within the European Convention on Human Rights (ECHR) and the International Covenant on Civil Rights (ICCPR) drawn up by the United Nations, it is not seen as an absolute right under English Law. Instead, it is governed by a series of Laws which are illustrated in **Table 2** .

The main restrictions to freedom of speech and the use of E-mail are, therefore, related to instances where it is in conflict with; company security, racial hatred, defamation, blasphemy and religious hatred, the distribution of obscene material and the infringement of an individuals' right to privacy. Issues which can be addressed to a large degree by defining permissible behaviour and clearly outlining disciplinary procedures within a policy document.

Privacy is 'the right of any person to be protected from intrusion upon himself, his home, his family, his relationships and communications with others, his property and his business affairs' (Collins & Murroni, 1996; pp.110).

As with freedom of speech, privacy is a human right but not one which is protected under English law except in relation to the Data Protection Act 1984 (and 1998). This gives individuals rights regarding personal information held on computer data bases or other automatic processing systems. Therefore, an E-mail policy needs to be far reaching enough to comply with the company's data protection registration and incorporate the principles of privacy, illustrated in **Figure 2.**

2.1.1 Ethics

Ethics refers to 'the principles of right and wrong that can be used by individuals acting as free moral agents to make choices to guide their behaviour' (Laudon & Laudon, 1997; pp.139). Although, a detailed philosophical discussion is not considered appropriate, it is necessary to have an overview of the widely cited ethical principles, as they pose unique challenges for individuals, organisations and society as a whole.

The basic concepts involved with the ethics of using and managing information technology are; responsibility, accountability, liability and due process. Concepts which are usually guided by company mission statements (Bankowski, 1997).

Table 1 - Legal Considerations

Companies Act 1985	All external E-mails should contain the name and address of the registered office and the company registration number.
Civil Evidence Act 1995	Allows for E-mail to be used as evidence in the event of a dispute. A company's storage strategy should be a suitable compromise between holding the least amount of data yet still complying with legislative and commercial requirements.
Data Protection Act 1984 (& 1998)	Users must ensure that the processing of personal data conforms to the company's data protection registration.
Interception of Communication	Employees must be informed that the company reserves the right to monitor the content of E-mails if necessary. Monitoring messages without prior statement of this intention could render the company liable under this Act.

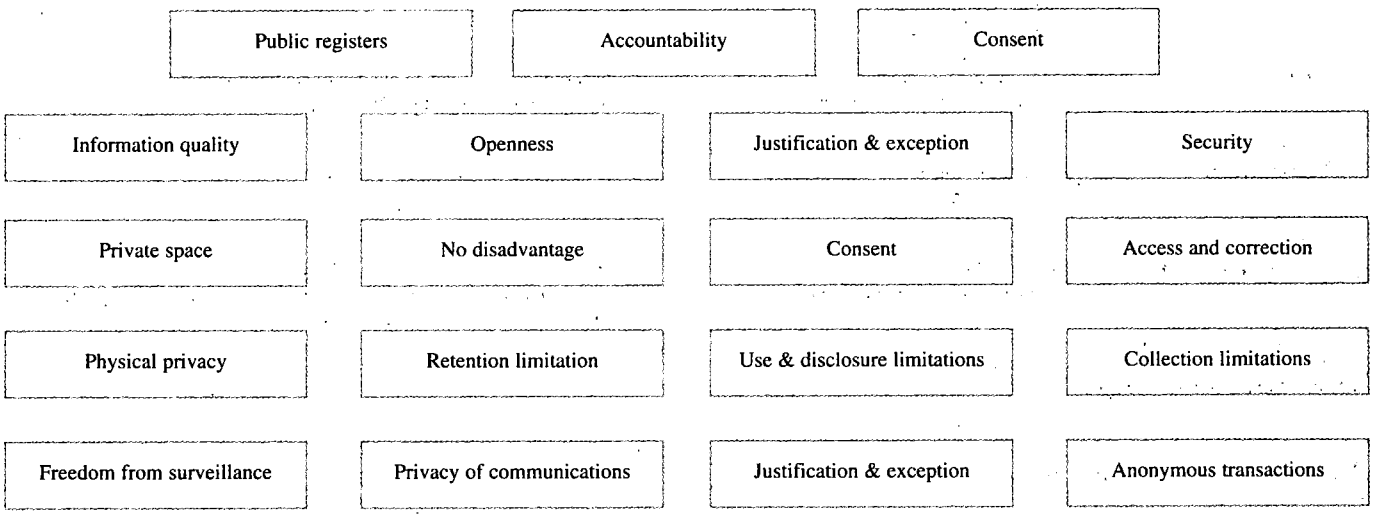
Taken from Association of British Insurers (1998; pp.1-3).

Table 2 - Laws & Statutes Applicable to the Content of E-mails

Obscene Publications Act 1959 & 1964
Indecent Displays Act 1981
Contempt of Court Act 1981 (revelation of sources)
Police and Criminal Evidence Act 1984 (revelation of sources)
Video Recordings Act 1984 (video classification)
Race Relations Act 1965, then Race Relations Act 1976 and now Public Order Act 1986 (incitement to racial hatred)
Malicious Communications Act 1988 (material distributed by mail)
Official Secrets Act 1989
Prevention of Terrorism Act (Temporary Provisions) 1989 (revelation of sources)
Broadcasting Act 1990 (notably in Section 10)
Football (Offences) Act 1991 (indecent or racist chants)
Criminal Justice and Public Order Act 1994 Forgery & Counterfeiting Act 1981
Copyright, Designs & Patents Act 1988
Data Protection Act 1984 (and 1998)

Adapted from Collins & Murroni (1996; pp.94-95); Zorkoczy (1990; pp.146).

Figure 2 - Principles Relating to Privacy



Adapted from Collier (1995; pp.44-45).

As technology improves and the capabilities of E-mail increase, new ethical problems will be encountered 'because most of the people that cause the problems do not understand the full implications of their actions' (Thomas *et al.*, 1998; pp.5). For this reason, a policy document should advocate procedures aimed at encouraging ethical behaviour and provide a framework for analysing future 'situations' ethically.

2.1.2 Security

Within most companies the security of E-mail systems tends to rely 'upon users mutual respect and honour, as well as their knowledge of conduct considered appropriate to the network' (Ratnasingham, 1998; pp.1). The main drawback of this approach, as Prasad *et al.* (1991) identified, is that people commit computer crimes not computers and 'the motivation for much computer abuse is retaliation against management'(pp.31).

The main security risks within an E-mail system have been identified as being; the availability and integrity of the information, the possibility of repudiation, difficulties in assuring confidentiality and authentication as well as controlling access to the system (Ratnasingham, 1998). Each of which has wide ranging consequences involving both direct and indirect losses.

For security risks to exist, there have to be weaknesses within the system. These weaknesses can occur at any one of six points; on the client side, at the user/computer interface, the post office, the gateway, the administrator or on the wire as **Table 3**, demonstrates.

To overcome these weaknesses within an existing E-mail system there are five basic goals which need to be achieved; certified delivery, protection against forgery and impersonation, message integrity, efficient and continuous information exchange and user protection (Gluck, 1994). Goals which can also be used to assess the security of new or proposed systems.

Attaining these goals and overcoming or at least reducing the security risks can be achieved by implementing a number of controls which fall into one of four classes; deterrents, detective, corrective or preventative controls, as described in **Table 4**. Each of which can be approached from either the technical, personnel/management or legal perspective (Baskerville, 1988).

Table 3 - Security Weaknesses Within an E-mail System

LOCATION	DESCRIPTION	WEAK POINT
Client side	The software and hardware used to compose, send or receive message.	Unattended PC's Lost or stolen mobile PC's Use of public transport service Temporary storage of sensitive messages
On the wire	Network carrying the message	No protection while being transmitted
The post office	The server which temporarily stores the messages until read, saved or deleted by the recipient.	User access Exposed user-Ids
Gateway	Takes messages created internally & passes them to the Internet	Encryption is not a viable option and therefore, the unprotected text presents an opportunity for eavesdropping and compromise.
Administrator	Person responsible for the integrity of the system	Can log-in, peruse or copy messages
User/computer interface	The interface between the computer and User (keyboard and monitor)	No method to positively identify the sender No protection against sending message to unintended recipient No provision to ensure the integrity of the message

Adapted from Gluck (1994; pp.28-30).

Table 4 - Classes of Control

CLASS OF CONTROL	DESCRIPTION
DETERRENTS	Strength of an organisations policy. Relatively inexpensive and reinforces controls.
PREVENTATIVE	Reduces the risk of occurrence - represents the first line of defence.
DETECTIVE	Identify the occurrence of harm within the information system. Raises awareness and for action to be taken. but does little to insulate the system by providing a solution.
CORRECTIVE	Minimises the effect of the threat after the loss has occurred but does little to prevent the threat. Only aids in recovering or reducing the extent of the damage.

Adapted from Baskerville (1988).

From the technological point of view there are a variety of applications which are currently available including; encryption, digital signatures, message authentication and user identification and authentication. Indeed, many of the products on sale today have control devises incorporated into them, although they are generally not sufficient to provide the sole means of control (Ratnasingham, 1998).

The personnel/management perspective identifies the most important practices and procedures associated with maintaining or enhancing the security of a system as being; 'recruitment procedures, policies on the non-use/non-disclosure of confidential information; vacation and job rotation policies, segregation of duties, channels for addressing grievances, personnel review procedures, employment termination policies' (Grundy *et al.*, 1994; pp.24).

Ultimately, the level of security required for an E-mail system will be determined by the type of information which is being sent. If it is being used for business critical information then the security of the system is of major importance. On the other hand, if the majority of users are only sending casual correspondence to business colleagues or letters to friends, then the level of security required is less critical.

Without information relating to how E-mail is being used and the type of information being sent, it is important to investigate potential solutions for making both the system and the message secure even though the latter is more manageable and cost effective (Gluck,1994). The options for implementation outlined later provide suggestions for security procedures using all three perspectives; personnel/management, technical and legal.

2.1.3 Justification

Those managing E-mail systems constantly face the issue of changing, or upgrading existing systems to expand functionality, enable greater integration between existing software, meet changing business needs or mandatory requirements such as compliance with the year 2000 (Irani *et al*, 1998). It is therefore, very important for a policy document to address the issue of justifying the investment in IT and what follows is a brief insight into the different methods which can be used, along with their associated advantages and disadvantages.

Over the years many different ways of justifying investment in IT have been used. Traditionally these have concentrated on the direct costs associated with the purchase and implementation of the system and balancing these off against the financial benefits such as staff savings. Some of the most frequently used methods include; Return On Investment (ROI), Net Present Value (NPV), Internal Rate of Return (IRR) and payback. The benefits of which are that they are objective, relatively easy to use and many people, although not necessarily competent enough to calculate the figures, are familiar and comfortable with the concepts.

However, IT professionals are becoming increasingly unhappy with these quantitative accounting methods as they concentrate on the short-term financial aspects of any investment and fail to take account of the intangible benefits associated with the implementation of IT (Semich, 1994).

In addition, these methods also lack the ability to reasonably assess and monitor the investment in IT over time. Although, many take a 3 or 5 year view in terms of the life cycle of the technology, the benefits of end-user systems such as E-mail are extremely hard to identify and even more difficult to predict. This is because they tend to change the way people undertake their jobs, which in itself is a very gradual process affecting the whole of the organisation (Gunston, 1998). Changes which have also been found to be specific to individual organisations making generalisations and comparisons extremely difficult (Mahood, 1994).

Today, the central issue when justifying IT investment is not just how IT can improve the efficiency of the organisation, but also how can it increase its effectiveness by supporting the goals of the organisation (Sherwood-Smith,1991). This is particularly true in the case of E-mail where 'the original justification of many organisations . . . [*was*] . . . to increase the efficiency by providing faster and easier ways to move information around the organisation' (Gluck,1994; pp.30), rather than producing staff savings.

There are, however, very few tools for measuring intangibles and monitoring IT investments overtime. One framework designed by Hochstrasser (1992) and illustrated in **Table 5**, identifies the direct, indirect human and indirect organisational project costs. Using this method it has been estimated that intangibles can be up to four times the cost of tangibles when implementing IT and have often been cited as the reason for failed implementation (Hochstrasser, 1992).

Ultimately, although, financial justification is needed to persuade organisations to invest in technology, it is not the technology which is of primary importance but how it is used. Therefore, rather than concentrating solely on the financial benefits associated with any investment it is proposed that attention and resources should also be allocated to determining exactly how, when and why individual users would benefit from any improvements to an existing system.

2.1.4 Policies Distributed on the Internet

The majority of the policies found by searching the Internet originated from either American educational establishments or from software suppliers. The scope and details of the policies varied enormously although, definitions of responsibilities and acceptable/unacceptable behaviour were generic to all policies. A summary of the main areas incorporated into the different policies is given in **Table 6**.

2.2 Case Study - Norwich Union

Norwich Union were involved in a highly publicised legal action involving the content of an E-mail sent internally by a Norwich Union employee and which subsequently came to the attention of Western Provident. This was the first such case to occur within the UK and the judge ruled the E-mail constituted defamation and awarded Western Provident £450,000 damages.

2.3 Summary of Main Findings

The literature review identified that any company was liable for the content the messages contained within any system owned, operated or subscribed to by the company. The liability extended to copyright and any loss of revenue or damaged incurred by another individual or organisation as a result of receiving a virus via an E-

mail sent using the system. To reduce it liability the company needs to comply with a number of legal obligations, clarify acceptable and unacceptable behaviour as well as distinguish between the responsibilities and accountabilities of individuals and the organisation. Issues which could be approached from a combination of personnel/management, technological and legal perspectives.

These findings, summarised in **Table 7**, were used to produce a draft policy document, design a series of options and develop a process for their successful implementation. Details of which are discussed in the next section.

Table 5 - Project Costs Associated with the Implementation of IT

COSTS	EXAMPLES
	DIRECT PROJECT COSTS
Environmental operating costs	Air conditioning facilities Uninterrupted power supply Computer furniture
Initial hardware costs	File server Terminals Network printer
Initial software costs	Software packages Operating system Networking software
Installation and configuration costs	Management consultancy support Installation engineers Network wiring, junctions and connectors
System development costs	External customising time In-house customising time
Project overheads	Running costs; electricity, space Networking costs: telecommunication time Rises in insurance premiums
Training costs	Vendor software familiarisation courses Software upgrading courses
Maintenance costs	Yearly service contracts
Unexpected hardware costs	Secondary data and storage devices Upgrades in processing power
Unexpected software costs	Vendor module software upgrades Operating systems upgrades
Security costs	Protection against viruses and abuse
Consumable	Print cartridges/ribbons, disks and paper
	INDIRECT HUMAN
Management/staff resources	Integrating new systems into new/revised work practices
Management time	Devising, approving and amending IT and manufacturing strategies
Management effort and dedication	Exploring the potential of the system
Employee time	Absorbing the transition from traditional to new work practices
Employee training	Being trained and training others
Employee motivation	Interest in IT implementation reduces as time passes
Changes in salaries and structures	Promotion and pay increases based on improved employee flexibility
Staff turnover	Increase in recruitment costs; interview, induction and training costs
	INDIRECT ORGANISATIONAL
Losses in organisational productivity	Developing and adapting to new systems, procedures and guidelines
Strains on organisational resources	Maximising the potential of the new technology through integrating information flows and increasing information availability
Business process re-engineering	The redesign of organisational functions
Organisational restructuring	Covert resistance to change

Taken from Hochstrasser (1992; pp.27-28).

Table 6 - Summary of the Content of Policies Distributed on the Internet

Purpose	◆ To enable the company to derive benefit's of increased efficiency through the use of E-mail while ensuring the protection of information assets, integrity and employee rights.
Scope	◆ To establish rules and procedures on the access and proper use and administration of electronic communications via E-mail and bulletin boards. ◆ More specifically, to define user responsibilities and liabilities e.g. virus checking attachments, password protection, archival/storage of old messages, use of distribution lists. ◆ Applicable to all employees, temporary, part time or agency staff and company owned or operated E-mail systems, or E-mail systems which are subscribed to and paid for by the company
Acceptable Use	◆ By employees of company. ◆ For business communications to conduct company business. ◆ Incidental and occasional personal use but messages become the property of the company and are subject to the same conditions as company E-mails.
Unacceptable Use	◆ For illegal purposes. ◆ For transmitting threatening, obscene or harassing material. ◆ To interfere or disrupt users by wilfully or maliciously degrading the performance of the network. ◆ Using the system to obtain unauthorised entry into another system.
More specifically:	
Security	◆ Circumventing user authentication. ◆ Interfering with users access. ◆ Forging or interfering with E-mail or header information. ◆ Using system to collect, retrieve or read messages sent to another user.
Privacy	◆ Respect the privacy of users. ◆ Sending large numbers of unsolicited mail or attempting to add addresses to any mailing list without prior positive consent from individual. Sending inappropriate messages
Freedom of speech	◆ Engaging in harassment whether through language, frequency or size of messages. ◆ No commercial messages, employee solicitations, messages of a political or religious nature are to be distributed using company E-mail.
Legislation	◆ Disclaimer: In no event will the company be liable to any customer or third party for any direct, indirect, special or other consequential damages for actions taken pursuant including, but not limited to, any lost profits, business interruption, loss of rams or other data, or otherwise, even if the company is advised of the possibility of such damages. ◆ Company is not responsible for content. ◆ Protect the legal copyright, licence and other legal devises to programs, communication and data. ◆ Company cannot guarantee that the E-mail communications are private, confidential or free from legal consideration. ◆ Individuals responsible for messages transmitted under their user ID and their compliance with law.
Ownership	◆ E-mail equipment and messages are company property. ◆ Messages that are created, sent or received using the company's E-mail are the property of the company. ◆ The company reserves the right to access and disclose the content of all messages created, sent or received using its system.
Bulletin boards	◆ Are for business related activities only. ◆ Procedure required to request authorisation to create a bulletin board. ◆ Responsibility of posting items on the BB.

Table 6 continued - Summary of the Content of Policies Distributed on the Internet

Retention Guidelines and requirements	◆ What is a record - namely, records include not only the messages sent and received but also the transmission and receipt data as well. ◆ How long should it be kept. ◆ All correspondence which exceeds the capacity of the mailbox will be deleted without notice. ◆ Those taking extended vacations or maturity leave, sickness must notify in writing the systems administrator.
Other areas	◆ Restrict use of 'copy all' for sending and responding to messages. ◆ All E-mail messages older than 30 days or undeliverable E-mail will be both removed and purged from the system. ◆ Unsolicited bulk E-mail.
Violation of Policy	◆ Employees should report any misuse of E-mail or violations of this policy immediately to ..... ◆ The company will make every effort to maintain confidentiality within the limits of other obligations. ◆ Reviewed on a case-by-case basis. ◆ Enforcement: the company may, in its sole discretion, suspend or terminate a user for violation of the policy at anytime without warning.

Table 7 - Summary of Findings

(Company name) .... is liable for the content of all E-mails contained on systems owned, operated or subscribed to by the company.

The operation of an E-mail system should comply with UK Law and International Law wherever possible as messages can be transmitted across national boundaries.

The policy document should:

ADVOCATE:

1. The principles of privacy.

2. Ethical behaviour and provide a framework for analysing situations ethically.

3. Reducing security risks by implementing a number of; deterrents or detective, corrective or preventative controls which can be approached from technical, personnel/management or legal perspectives.

4. Resources being allocated to determining exacting how, when and why individual users would benefit from any improvements to an existing system as well as financial justification.

STRUCTURED TO INCLUDE:

1. Statement of purpose, ownership and intention to monitor E-mails.

2. Definition of acceptable and unacceptable behaviour in terms of security, privacy, freedom of speech and current legislation.

3. Retention guidelines and requirements.

4. Consequences of policy violation

3. Options for Implementation

To simplify the process of designing a policy which incorporates all the issues, principles and findings from the research, a number of existing frameworks have been used which were identified while researching this project. The benefits of adopting this approach are not only the savings made in time, money and effort but also the ease and efficiency with which such frameworks could be incorporated effectively into existing training programmes and procedures within the company.

Detailed below are a series of options which have been grouped into four broad categories; options aimed at addressing current legislation, those associated with the management of the system, amendments to personnel policies and practices, a draft policy document and proposals for finalising the policy content and the implementation process.

3.1 Complying with Legislation

The priority must be to ensure that the system complies with current legislation both here and abroad as E-mails can cross national and international boundaries. To do this:

1. An individual should be made responsible for keeping abreast of legislative issues and making amendments to the policy, personnel practices and procedures as well as the management of the system, when required.

2. The system should be set-up to issue a statement automatically at the end of every message which gives the name and address of the registered office along with the company's registration number in order to comply with the Companies Act 1985. It also needs to contain a paragraph similar to that used by PricewaterhouseCoopers and illustrated in Figure 6.1 overleaf, to address Copyright Laws.

3. To comply with the Interception of Communication Act 1985, the company must also notify users of its intention to monitor E-mails contained on systems owned or operated by the company. Whether this monitoring is actively undertaken, or occurs passively through regular maintenance of the system is immaterial, users must be informed of the company's intention to screen messages.

4. The company needs to draw up and issue company guidelines on the storage of E-mails as the Civil Evidence Act 1995 allows that any message can be used as evidence in the event of a dispute.

5. Employees must be made aware of the rules and regulations governing the use and storage of personal information in accordance with the Data Protection Act 1984 and 1998 in order to comply with registration requirements.

3.2 Management of the System

◆ **Consider Partnerships**

Rather than continue to provide a full in-house service to all users, the company could investigate the feasibility of partnerships with suppliers who posses the skills, knowledge and experience of running a company E-mail system. For example, a partnership with a specialist agency working in the field of computer policing could overcome the skills shortage, as well as guarantee the independence of the policing mechanism and remove any accusation of the company spying or prying on its employees.

◆ **Obtaining Information from the System**

Simple analysis of when the system is being used, the volume of messages being sent, the nature and frequency with which faults occur, can make an enormous difference to the ease and predictability of maintaining a system.

◆ **Security of the System**

Although, laws and company policies can define and facilitate the legal and ethical use of computers 'people often act without considering the effects of what they do'(Thomas *et al.*, 1998; pp.5). Therefore, there is a need to develop 'built-in' procedures which wherever possible prevent data theft and piracy. There are many ways in which technology can be used to facilitate the security of an E-mail system. Although, many of the examples referred to in **Table 8**, are likely to already exist it is important to revisit and/or reacquaint users and Managers of the system with these items and review them on a regular basis.

In addition, further options could be considered such as limiting the size or format of the information and restricting access to particular websites making it harder for information to be sent and received via E-mail. Also, scans of information coming into and out of the company could be regularly undertaken to enable jobsites, jokes and pornography to be detected and blocked. The more automated these intervention procedures are the more effective and reliable they are likely to prove.

Table 8 - Good Security Procedures

◆ User ID's and passwords.

◆ A policy with particular reference to; minimum length, guidelines as to what constitutes a secure and proper password as well as the frequency with which it should be changed.

◆ Fit all PC's with an intermission lock-out capability which activates when computer not in use for a given period of time.

◆ Have separate people and duties for the roles of post office and LAN administrators.

◆ Grant minimum access rights to all users and administrators.

◆ Physically secure the post office server and its console along with any 'gateway' systems.

Adapted from Gluck (1994) and Grundy et al, (1994; pp.16).

3.2.1 Justification

Ultimately, financial justification is needed to persuade organisations to invest in technology. However, it is not the technology which is of primary importance but how it is used which matters. Therefore, rather than concentrating solely on the financial benefits associated with any investment it is proposed that resources are also allocated to determining exacting how, when and why individual users would benefit from any proposed improvements to the current system.

◆ **The Internet**

It is possible to argue that access to this facility should be restricted. Alternatively, the connection to the Internet could be managed in a way which is similar to the bar on international dialling. Namely, only allowing Internet access in instances where a business case can be proved. This is considered sensible and expectable practice for the telephone so, why not for E-mail?

3.2.2 Enhancing Service Provision

Other options recommended for implementation and aimed at increasing the perceived level of service are detailed below:

1. *Undertake a Communications Audit*
2. *Create Effective Communications*
3. *Develop and Implement User Focus Standards*
4. *Investigate Tailoring the Service to the User*
5. *Restrict the use of the 'Copy all' facility*
6. *Remove automatic receipt facility*

3.3 Personnel Policies and Practices

The third group of options incorporate amendments or additions to personnel policies and the working practices of employees of the company. They include; addressing the issues of copyright, privacy, ethical use and security practices.

3.3.1 Copyright

A simple amendment to the standard Contract of Employment and signed by all employees would effectively overcome the problem of copyright. The statement must confirm that the individual agrees not to breach copyright laws and gives permission for any information they produce to be used by others within the company.

3.3.2 Privacy

One example of an existing framework is the OECD's (1990) Guidelines on the Protection of Privacy and Trans-boarder Flows of Personal Data. By simply inserting 'E-mail' in place of 'data' the framework can be adapted very easily to the use of E-mail as **Table 9** demonstrates. A framework such as this should be included in any E-mail policy and employees encouraged to adopt it as standard practice.

Table 9 - OECD's (1990) Guidelines on the Protection of Privacy and Trans-boarder Flows of Personal Data Adapted for the Use of E-mail Within an Organisation

1. The purpose for which information contained within an E-mail is required should be identified before the information is collected and the information collected should be limited to that necessary for the identified purpose.
2. Those to whom information contained within an E-mail relates should be aware of and consent to its collection, use and disclosure.
3. Information contained within an E-mail should be processed fairly and lawfully.
4. Information contained within an E-mail should not be used or disclosed in a manner incompatible with the purpose for which it was collected, except with the consent of those to whom it relates.
5. Information contained within an E-mail should be complete, accurate, relevant and up-to-date to the extent necessary for the purpose for which it is to be used.
6. Information contained within an E-mail should not be held longer than is necessary.
7. Those to whom information contained within an E-mail relates should have access to information concerning them and be able to have incorrect information updated or deleted.
8. Business information should be protected against unauthorised access, or alteration, disclosure or destruction and against accidental loss or destruction.
9. Someone should be made accountable for compliance with the above principles.

Adapted from OECD Report (1990; pp.235).

3.3.3 Ethical Use

It is always preferable to prevent 'situations' from occurring rather than solving them once they have occurred. Therefore, by providing employees with information which encourages them to use E-mail ethically it is anticipated that fewer 'issues' will arise. A simple approach advocated by Thomas *et al.* (1998) and aimed at encouraging ethical behaviour is outlined in **Table 10.**

Table 10 - Procedures Aimed at Encouraging Ethical Behaviour

Develop a corporate guide to computer ethics for the organisation;

Develop a computer ethics policy to supplement the computer security policy;

Adding information about computer ethics to the employee handbook;

Finding out whether the organisation has a business ethics policy, and expanding it to include a computer ethics policy;

Learning more about computer ethics and spreading what is learned;

Helping to foster awareness of computer ethics by participating in a computer ethics campaign;

Making sure the organisation has a electronic mail privacy policy;

Making sure that employees know what the electronic mail privacy policy is.

Taken from Thomas et al. (1998; pp.5).

As technology develops new ethical problems will undoubtedly arise. Therefore, a framework such as that given in **Table 11**, is needed to ensure that when these 'situations' do occur, they are analysed and dealt with ethically.

Table 11 - A Framework for Analysing Situations Ethically

1. Identify and describe clearly the facts
2. Define the conflict or dilemmas and identify the higher order values involved
3. Identify the stakeholders
4. Identify the options that can be reasonably taken
5. Identify the potential consequences of these options

Taken from Laudon & Laudon (1997; pp.144).

3.3.4 Security Practices

Although, the overall level of security within any E-mail system can be enhanced through the application of technology, ultimately, it comes down to the actions of individuals. Illustrated in **Table 12** are examples of the type of procedures which could be implemented to encourage good practice within an organisation.

Table 12 - Security Procedures - A Human Resource Perspective

A HUMAN RESOURCE PERSPECTIVE:

- Careful selection of staff with due regard to their honesty and integrity.
- The raising of computer awareness among staff and ensuring that staff are aware of the company's security policies.
- Methods of tackling the personnel problems of staff which might lead them into the crime abuse e.g. advocating referring employees with difficulties to properly run employee-assistance programmes.
- Access how effective grievance procedures are since as Prasad et al (1991) pointed out the motivation for much computer abuse is retaliation against management.

Adapted from Gluck (1994) and Grundy et al. (1994; pp.16).

Another source of useful and relevant information is the work of Ratnasingham (1998) shown in **Table 13.** Although, originally proposed as guidelines for secure electronic commerce they are, on the whole, equally applicable to the day-to-day use of E-mail.

Table 13 - Guidelines for Secure Electronic Commerce

- Customers are individually responsible for understanding and respecting the security policies and are individually accountable for their own behaviour.
- Have the responsibility to employ available security mechanisms and procedures to protect their own data.
- Administrators are responsible for maintaining the security of the system which they operate and also to notify customers of their security policies.
- Software systems and developers are responsible for providing systems which are sound and embody adequate security controls.
- Customers, service providers, hardware and software vendors are all responsible for co-operating toward providing a secure environment.
- Technical improvements in the Internet service protocols should be sought on a continuing basis.

Taken from Ratnasingham (1998; pp.4).

3.4 Draft of Policy Document

Drawing heavily on the findings from the research including examples from the Internet and the British Associate of Insurers, it was possible to draft a policy for the use of E-mail, see **Table 14.** This document not only needs to be finalised to meet the individual needs of an organisations but also to be supported by a company's personnel policies and practices as well as its overall management system.

Table 14 - Draft of Policy Document

E-MAIL POLICY

Purpose:

To outline the rules and regulations governing the use of E-mail systems owned, operated or subscribed to by the company. By designing and implementing a policy, the company is aiming to protect employees' rights and enable the systems to operate legally, ethically and securely.

Acceptable use:

The E-mail systems, including bulletin boards, must only be used by full, part-time or temporary employees of the company, including agency staff, for business purposes only. (definition required).

Unacceptable use:

For illegal purposes including infringement of copyright and the distribution of pornography, containing threatening or harassing material, attempting to degrade the performance of the systems or infringing User authentication or privacy rights.

Responsibilities of individual users:

- To read, understand and enforce the company policy.
- To uphold the integrity of the security procedures implemented by the company including user ID's, passwords and gaining unauthorised access to areas of the system.
- Individuals are responsible for all messages transmitted or received under their User ID including undertaking appropriate virus checks on all messages and any attachments.
- To store E-mails in compliance with company's retention guidelines and thereafter, the removal of messages.
- To notify Administrator of extended absences e.g. sickness, maternity leave.
- To obtain positive prior consent from individuals before adding them to mailing lists or using information collected by or relating to them.
- Report any violations of the policy to the Systems Administrator immediately.

Violation of policy:

Will result in an investigation of the incident and if the violation is confirmed disciplinary action will be taken which could result in dismissal or legal action.

The company is not responsible or liable for the content of any E-mails and cannot guarantee that a message will remain private, confidential or free from legal consideration. The company retains the right to monitor, intercept and disclose the content of any E-mails sent or received, all of which are the property of the company.

This policy is effective from . . . . . .

4. Implementation

The introduction of policies or procedures involving the use of technology and indeed the implementation of the technology itself is, often associated with a 'big bang' image even though it involves a process of change rather than a single event. This is particularly true where the aim is to implement a policy outlining the acceptable use of an existing E-mail system rather than introducing new technology.

It has been proposed by Clark *et al.* (1988), building on the work of Wilkinson (1983), that technological change involves five

Table 15 - Stages of Technological Change as proposed by Clark et al. (1988)

Stage	Description
INITIATION	The process by which Managers identify and pursue an opportunity for the adoption of policies associated with the use of technology.
DECISION TO ADOPT	Refers to the process leading up to the decision to invest resources in the formulation and introduction of technology and/or policies associated with its use.
POLICY SELECTION	Denotes the process of in-house design and development of a particular policy.
IMPLEMENTATION	Embraces the process of introducing policies into the workplace. This includes both technical and human aspects of formulating, commissioning and 'debugging' the chosen policy and the 'mediating' role of management and union strategies towards its implementation.
ROUTINE OPERATION	Is where the policy has been brought into service and aa stable pattern of working within its guidlines and recommendations has been established.

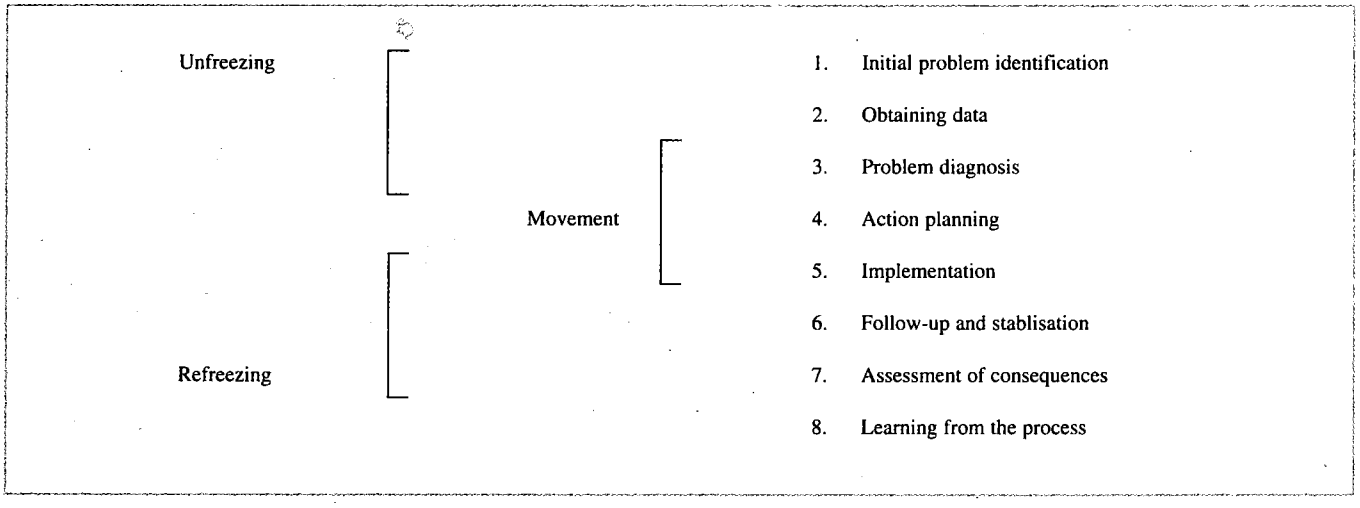
Adapted from McLoughlin & Clark (1996, pp. 59-60).

distinct stages; initiation, decision to adopt, system selection, implementation and routine operation. A five stage process which can easily be adapted to the implementation of a policy associated with the use of technology, as **Table 15** illustrates.

Although, this model incorporates the 'temporal' aspects of policy formulation and provides a sequential analysis of the process of implementation, the model as a whole is not without its critics (e.g. Dawson, 1993). Rather than dismiss Clark's model with its useful definition of the five stages of implementation, it is perhaps of greater benefit to combine this model with a more 'human' approach to change. For example, according to French et al (1985), change involves a planned three-stage approach; *unfreezing* elements which are maintaining the present system, *movement* to adopting or accepting new attitudes and beliefs and finally *refreezing* at a predetermined point by enforcing policies, structures and norms which serve to reinforce the change. These three stages were broken down further to provide eight elements for a planned change and these are shown in **Figure 4.**

Using these two models as guidelines, detailed in **Table 16** & **Figure 4**, are the actions required for change within each stage and

Figure 3 - Stages in Planned Change Effort

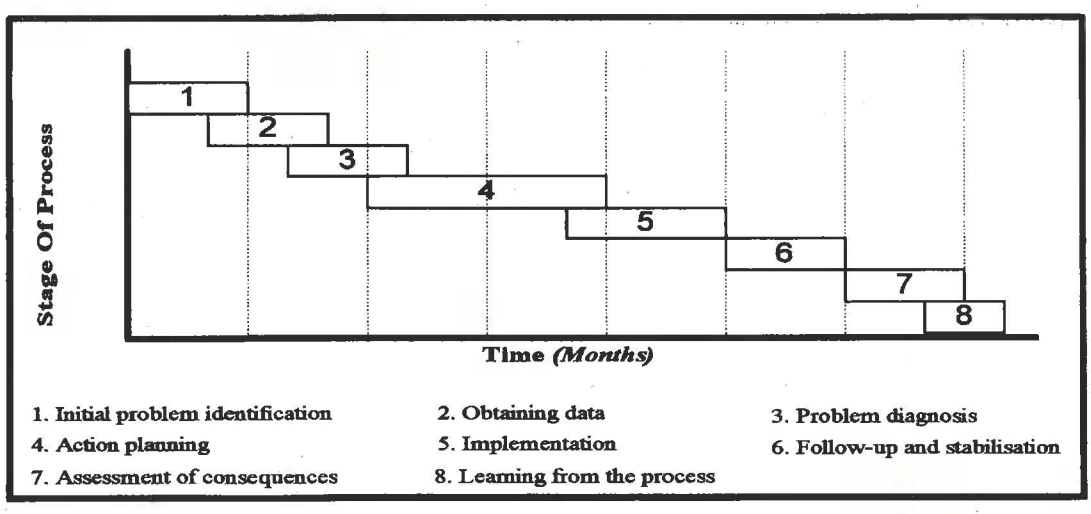


Taken from Mullins (1985, pp. 500)

Table 16 - Actions For Implementing Change

ACTION	DESCRIPTION
Initiation	Discussions to notify all involved of the aims & objectives, along with the proposed program of events with the aim of gaining support and agreement. These discussions will also provide the opportunity to expand the different options, assimilate suggestions and make any necessary amendments to the policy as well as the implementation plan.
Decision to Adopt	Prepare & present a paper to the Board to obtain consent.
Policy Selection	Conduct a detailed examination of the consequences of the proposed policy in terms of cost, most appropriate hardware & software, training requirements, amendments to personnel policies, detailed timings and implications for the future.
Implementation	Design & test policy and begin the training & communication programme. Time to 'iron-out' any last minute issues ready to go 'live'. Implementation of policy.
Routine Operation	Follow-up and stabilisation period.
Assessment of consequences	Discussions with all concerned.
Review of learning from process	Discussions with all concerned.

Figure 4 - Actions & Timetable for Implementing Change



a timetable for the change process. Although, not every element of the implementation process can be either controlled or planned it is believed that this action plan could help increase the likelihood of successful implementation.

The previous section outlined a series of options for implementation and although it was recommended that all the options are considered the actual process of implementation would contain similar characteristics irrespective of the number or combination of options finally adopted.

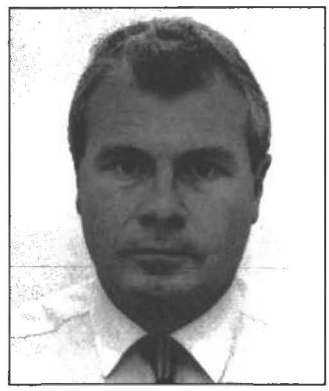
5. Conclusions

E-mail is a powerful and easy to use communication tool, but like the Internet its use is in danger of becoming out of control. Increasing proportions of company's IT budget are being used to support and maintain the E-mail system. The overall objective of the paper was to design, develop and document the process which could be used to formulate a policy relating to the use of E-mail. A policy which would protect the security and integrity of the company's information assets and the rights of individuals using the system.

By examining E-mail policies developed and implemented by other companies, exploring the managerial issues associated with the use of E-mail a series of options were developed and process designed for their implementation. As well as providing a draft of a policy document these options, which incorporated technological, personnel, management and legal perspectives, provides a framework which utilises 'best practice', identifies the responsibilities of a company and the individuals using the system, provides guidelines as to specific requirements, possible standards and levels of compliance.

A policy which needs to be continually updated to accommodate the changes which will undoubtedly occur every time a proverbial stone is thrown into a pond.

REPORT FROM THE CASH BOX



Mike Demetriou
Treasurer

Commentary

The group made a loss for the year of £1,833 from its activities.

There was a continuation of the trend of a decline in membership. Technical briefing income appears good against last yearís figures but there are some outstanding expenses due which will alter this position slightly. Additionally there were administration costs from 1997/8 that were not received until the following financial year and these effectively put us into the red.

Our cash balances are still very healthy at £37,570 and the committee is actively looking for ways of productively using these. If you have any constructive ideas for utilising these funds please contact the Chairman John Bevan.

Income and Expenditure Account for the Year Ended 30 April 1999

Income	**1998/1999**	**1997/1998**
	£	**£**
Technical Briefing Sessions & other meetings	10,156	8,604
Subscriptions	4,225	5,135
Interest on Bank Accounts	1,362	1,378
Journal Advertising	293	500
Other Income	5	18
Prior Year Items		252
	16,041	15,887
Expenditure		
Technical Briefing Sessions & other meetings	6,274	7,759
Journal	5,148	4,876
Printing, Postage & other Administration Expenses	3,489	1,288
Prior Year Items	2,963	
	17,874	13,923
Profit/Loss for the Year	(1,833)	£1,964

Fund Balance	**£**
Fund Balance at 1st May 1999	39,403
Add 1998/99 loss	(1,833)
Fund Balance at 30 April 1999	37,570

BCS MATTERS!

Colin Thompson
BCS Marketing Director

Awards for BCS Members

News of important awards for two senior members of the BCS security community. Firstly, Ron Middleton who received a lifetime Achievement award at the Secure Computing Dinner, held to coincide with the InfoSecurity exhibition in April. Ron spent 36 years with the Bank of England before his retirement and has been a member of the BCS Security Committee for many years.

The second award is that of Honorary Fellowship to Willie List. As many readers will know, Willie worked tirelessly for the Society up to the time of his heart attack last year. He still manages to make a significant contribution although he is now restricted by ill health. The Honorary Fellowship was approved by Council in May and is due to be presented to Willie at a lunch to be held in early July.

And more Awards

This time, the BCS Management awards. The final stage of the 1999 event involved three short listed organisations - the Automobile Association, Transco and Hammonds Direct. The winners, announced at a dinner on 12 May were the AA for their AAHelp system that has enabled the organisation to reduce from eight call handling and deployment centres to three, cutting costs by a third, whilst also achieving a significant improvement in response times to customers.

BCS Membership

I have mentioned BCS membership issues in previous issues of this newsletter, particularly in relation to the changes proposed by Alan Pollard's Working Party last year. Work is now moving forward on a number of fronts, including the implementation of the Review where A four-year implementation programme has been initiated. The work will be overseen by a steering committee of six senior members, chaired by the President-Elect David Hartley,

Urgency is being given to improving the access to BCS qualifications for the current BCS professional community. In the first year the work will be focused on reducing the minimum experience route, especially for the entry professional grade, Associate Member, which is currently four or seven years, depending on an applicant's academic qualifications.

In the second and third years the focus will switch to encouraging all IT staff into membership, in particular by creating the grade of Certified Affiliate to distinguish IT staff who do not yet qualify for professional membership from those Affiliates not professionally involved in IT.

Broadening the scope of membership to include those involved in the management and teaching of IT will also be an important part of this stage of the programme. Over the coming year the Society will be undertaking research to establish the requirements of this wider community.

In the meantime, moves to make joining the BCS as simple as possible have progressed with the launch of automated application and payment services on the Web site. New members can now complete a simple form and pay by credit card online. Alternatively they can download the form for printing and sending with payment by post.

Applying for upgrade to professional membership has also been simplified. A new, shorter application form is now being piloted and it is planned to eliminate the need for an interview where the paperwork, including sponsors reports, shows clear eligibility. These changes are intended to encourage more people to complete the application process and recognise that pressures of work now make it difficult for many professional to find the time to complete lengthy forms or attend interviews. The aim is to reduce bureaucracy without risk to entry standards and Membership Committee will be monitoring the implementation carefully to ensure that both objectives are met.

BCS Examinations

The Society is introducing a new syllabus and structure for its examinations. Based on a modular structure, there are now 3 stages - Certificate, Diploma and Advanced Diploma, replacing the existing parts 1 and 2. Further information on the new exam, and other subjects mentioned in this article, can be obtained from Customer Services at BCS HQ or from the BCS Web site (http://www.bcs.org.uk).

ISEB Certificate in Information Security Management Principles

The Society has awarded its first Certificates in Information Security Management Principles. The certificate is designed to provide candidates with a good knowledge and understanding of the general well-established techniques of Information Security. It is awarded to candidates upon successful completion of an examination written and organised by ISEB. Attendance on a recognised course is a pre-requisite for entry to the exam for all but the most experienced candidates. ISEB needs more organisations to offer training courses and is inviting applications from any organisation interested in becoming an accredited training provider.

New Publications

The BCS has published volume 4 in its Y2K, Practical Guides, series. The end of the millennium is almost upon us and time is running out for taking action to ensure a trouble free date change. This fourth book in the very popular series explains what can still be done to minimise risk and to maintain business continuity. The book is available from Customer Services at £15 for BCS members and £20 for others.

The Society is also active in the area of electronic publishing. The electronic Workshops in Computing (eWiC) series provides detailed information from leading edge, international workshops in computing science. Each publication is based on the proceedings of a specialist workshop and is designed to provide information that represents a "snapshot" of current knowledge, debate, or research. Each title in the series has an associated abstract booklet, which can be ordered electronically, or bought through standard outlets.

The full papers and multimedia resources of a workshop are provided on the BCS Website - access to which is gained by providing information contained within an

abstract booklet, or by providing a "Payment Code". A Payment Code can be obtained by making a credit card payment on the eWiC customer helpline. For further information, see the Website (http://www.ewic.org.uk/ewic/)

And a New Marketing Director

The old Marketing Director (and writer of this column) having moved on to do other things - including the implementation of the Membership Review mentioned above - the Society has recruited Alida Macchietto. Alida has an extensive Marketing career background, including some years spent in the publishing field. At the time of writing she is three weeks into trying to understand the complexities of the BCS!

And Finally.....

A date for the diary - the BCS Annual Dinner to be held at the Brewery in London on November 24. The Dinner is now very popular and we had a very full house at the Brewery last year. So, to avoid disappointment, contact Karen Jones on 01793 417434 or e-mail kjones@hq.bcs.org.uk. Karen will be happy to take your booking, either for individual places or for a company table.

Colin Thompson is Deputy Chief Executive of the BCS

So What About Students?

David Chadwick

Several universities and colleges around the country teach students about computer auditing. Most are business schools who teach it as part of a wider audit education for business courses but some are computing schools who teach it as part of information systems courses. Many guide students towards professional careers in auditing and towards preparing them for qualifications such as CISA and QiCA. For instance, we, at the University of Greenwich, for students on our BSc (Hons) Information Systems, provide 60 hours of tuition on auditing methods and security and legal issues associated with auditing. If assessments are passed at a high level the student is qualified for exemption from the Information Systems Auditing paper of the QiCA.

However, there are important elements to an education that academics are not able to fully give. Students need contact with professional bodies to learn about current issues; also with individual professionals working in the field who can give the personal dimension to the actual job. You wouldnít believe how difficult it is to obtain a speaker for a half-hour hour talk to 50 students. It is even more saddening when one looks at work experience for students. At Greenwich, the Information Systems degree is a sandwich course which means students attend a full-time work placement for 12 months and this is part of the degree award. The university and the students themselves have sought computer audit positions for such placements but to no avail. It seems few, if any, organisations are willing to give youngsters the opportunity to find out what the job is really all about. Research also is a sadly neglected area. Several universities have postgraduate students (MSc, MPhil and PhD level) who are researching issues of direct importance and practical use to the professionals in the field. At both Greenwich and the University of Wales there are research projects on spreadsheet errors and auditing, and Southampton Institute along with the University of North London are doing research into software quality management including standards and development issues that would affect auditors.

So, do you think that something should be done? Not quite sure what? Perhaps you've forgotten what the student experience is like. Then have a go at this examination !

Exam Title: Methods For Widening The Appeal Of CASG in Higher Education

Date: Today **Time: 5 minutes**

This exam is NOT open-book: no books or notes may be used – only common sense and intellect.

Please tick the answers that most closely match your own opinion.

Question 1: How well known is CASG amongst computer audit students in higher education?

a) CASG is a well known name in university schools of business and computing
b) CASG occasionally surfaces on student notice-boards and then disappears into oblivion
c) Most students think CASG means 'Computer Assessment of Sexual Gender'

Question 2: What can CASG do to widen its appeal to computer audit students in higher education?

a) It could provide names of practising auditors willing to give talks at universities
b) It could provide names of companies willing to accept students for work experience
c) It could provide support for computer audit research projects at postgraduate level

Question 3: What can I personally do to help CASG with this problem?

a) I will contact David Chadwick at University of Greenwich with my suggestions
b) I will contact John Bevan at CASG with my suggestions
c) I will do nothing

John Bevan and the CASG organising committee believe something needs to be done in this area ñ see Johnís thoughts in Chairmanís Corner. They are considering lowering the fees for students attending Technical Briefings along with a number of other suggestions. Why not let us know what you think and how we might go about doing things ? Many thanks.

David can be contacted by email at d.r.chadwick@greenwich.sc.uk or 0181 331 8509

British Computer Society

Management Committee

CHAIRMAN	**John Bevan**	**Audit & Computer Security Services**	**01992 582439** **john.bevan@virgin.net**
SECRETARY	**Raghu Iyer**	**KPMG**	**0171 311 6023** **raghu.iyer@kpmg.co.uk**
TREASURER	**Mike Demetriou**	**Lombard North Central plc**	**01737 776127** **mdemetriou@lombard.co.uk**
MEMBERSHIP SECRETARY	**Jean Brown**		**01803 872775** **100125.66@compuserve.com**
JOURNAL EDITOR	**John Mitchell**	**LHS Business Control**	**01707 851454** **lhs001@aol.com**
SECURITY COMMITTEE LIAISON	**John Bevan**	**Audit & Computer Security Services**	**01992 582439** **john.bevan@virgin.net**
TECHNICAL BOARD LIAISON	**Allan Brown**	**Consultant**	**01803 872775** **100125.66@compuserve.com**
TECHNICAL BRIEFINGS	**Jenny Broadbent**	**Cambridgeshire County Council**	**01223 317256** **jenny.broadbent@finance.cambscnty.gov.uk**
	David Cox	**Lombard North Central plc**	**01737 776286** **dcox@lombard.co.uk**
	Paul Plane	**National Westminster Bank plc**	**0171 726 1000**
	Alison Webb	**Consultant**	**01223 461316** **amwebbcam@aol.com**
ACADEMIC RELATIONS	**David Chadwick**	**Greenwich University**	**0181 331 8509** **d.r.chadwick@greenwich.ac.uk**

Membership Enquiries to:

Jean Brown
Whiddon Lodge
Abbotskerswell
Newton Abbot
Devon
TQ12 5LG

British
Computer
Society

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

Membership Application

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

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

CORPORATE MEMBERSHIP (Up to 5 members)* £75

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

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

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

BCS membership number: _____

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

Educational Establishment: _____ £10

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

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: (Please circle) 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)
SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS CASG"
AND RETURN WITH THIS FORM TO THE ADDRESS SHOWN ABOVE

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
PROFESSIONAL CATEGORY: 1 = Internal Audit 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)