ISSN 0961-9348

casg
Computer Audit
Specialist Group

JOURNAL

BCS

VOLUME 11 NUMBER 3 SUMMER 2001

Programme for members' meetings 2001/2002 season

Tuesday 2nd October	**Windows 2000 Security** *Configuring NT securely is often a major hurdle - Windows 2000 adds many new challenges to a secure infrastructure. Risk minimisation strategies include: reviewing typical threats; using W2K security mechanisms pro-actively; customising administrative control; planning and implementing counter-measures securing Active Directory; the encrypting file system.*	Evening 16.00 for 16.30 KPMG
Monday 12th November	**Outsourcing & Out of Control Projects** *About 25% of software projects will be cancelled because they are late, over budget, have unacceptably low quality, or experience some combination of these problems. Outsourced operations have created new security threats and risks. Practical control measures are vital. The risks associated with outsourcing overseas and ecommerce operations will be considered.*	All Day 10.00 to 16.00 ICAEW
Tuesday 4th December	**Network Security & Management** *Changes in the technologies underlying computer networks are important to auditors because these have implications both for network security management and the audit of these arrangements. These implications provide today's theme concentrating by way of example on the audit of ATM (Asynchronous Transfer Mode) and Frame Relay.*	Evening 16.00 for 16.30 KPMG
Tuesday 29th January	**Internet Security** *The theme of the day will be internet security, but particularly Intrusion Detection systems. These are automated systems that monitor communications and operating systems, alerting operators of potential hacking attacks.*	All Day 10.00 to 16.00 Royal Aeronautical Society
Tuesday 12th February	**The Subversive Spreadsheet** *"A spreadsheet application can subvert all the controls in all other parts of an information system" (R. Butler, VAT Auditor, Customs & Excise). This talk by presenters from The European Spreadsheet Risks Interest Group shows the evidence. It discusses the risks, the audit and preventative methods*	Evening 16.00 for 16.30 KPMG
Tuesday 5th March	**The System's Down - Again** *The unavailability of computer systems can give rise to serious problems for the continuing operation of the business. The ability to deal with or prepare for these problems is critical for business survival. The theme of the day is how business minimises their risk and will include high availability options, problem management and business continuity.*	All Day 10.00 to 16.00 Royal Aeronautical Society
Tuesday 14th May	**Data & The Law** *The legal risks and issues associated with IT and networking are not always well understood and often underestimated. This update on a fast changing area of the law is aimed at meeting the needs of risk management/audit professionals and providing opportunities for debate and discussion.* **This will be followed by the Annual General Meeting.**	Evening 16.00 to 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 back page.

Contents of the Journal

Editorial Panel

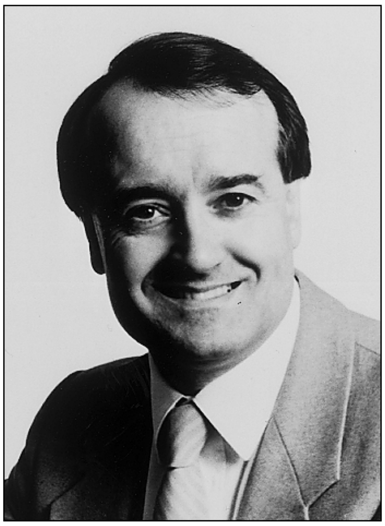
The **Journal** is the official publication of the Computer Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

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,
Tring, Herts.

EDITORIAL



With this edition of the *Journal* you should have received your renewal advice.

There are five types of renewal: corporate main, corporate subsidiary, individual, student and courtesy. The corporate main member pays a subscription that includes up to four other people at the same organisation. Corporate subsidiary members would be well advised to check that their main member is taking responsibility for payment. With transfers of staff and re-organisations it is easy to assume that action is being taken when it isn't! Individual renewals are of two types: BCS members and non-BCS members. The former get a cheaper rate. Full time students receive a special low rate to encourage them to take an interest in information systems auditing.

Whatever your membership level, please take a moment to renew your subscription. Not only does this entitle you to four copies of this *Journal* each year, but a scan of the list of either free, or heavily discounted events on the front cover should make you realise what a bargain this is. Subscriptions for other professional organisations often exceed one hundred pounds. Well, that's the drum banging over for another year.

This edition deals with a topic dear to my heart: the teaching by academia of good system design techniques by way of models seeded with errors for the student to find and comment on. I have often berated academia for not teaching control techniques so it is really wonderful to see the good work of Sue and Chadwick at Greenwich University represented in this Journal. This piece is complemented by Doherty and King's research into organisational issues in systems development projects and an analysis of BS7799 requirements for e-commerce by Gary Gaskell of the Bank of Queensland, Australia. Add to this Andrew Hawker's web page and Colin Thompson's update on what's happening with our parent body and you get an idea as to why you should renew your subscription (oh well, one last bang of the drum).

Have a good summer.

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 Teaching of Database Development using Error-awareness Methods for Improving Integrity

R.E.Sue and D.Chadwick.
Information Integrity Research Centre,
School of Computing & Mathematical Sciences,
University of Greenwich, London SE10 9LS, United Kingdom
Phone: 020 8331 8431 Fax: 020 8331 8665 Email:cd02@gre.ac.uk

Abstract

Businesspeople and auditors alike have consistently shown interest in reducing the incidence of errors in database models used in industry. In an attempt to reduce such errors, a teaching approach has been devised which includes the raising of student awareness to the common mistakes that occur during database development. The approach is based on the premise that teaching database development is too often based upon 'how to do things correctly' and seldom addresses 'how to avoid doing things incorrectly' and makes use of models seeded with deliberate errors which students are asked to find and comment upon. The approach is based upon similar successful outcomes using seeded models to combat spreadsheet errors. The overall result is that students are given a set of self-audit skills for error-checking that improve integrity of models during training and later during the work-place.

1.0 PROBLEM OF ERRORS IN END-USER APPLICATIONS

The problem of data integrity pervades the whole of an information system.

Over several years of teaching databases to students it has become apparent that each new intake of students tends to make the same errors as the year before. It was realized that better methods needed to be investigated that would aid the students in making fewer errors during database development.

A search was made for methodologies and tools available in industry that might be useful in an educational environment. A pilot investigation revealed that, in industry, large scale software developments by professional computing staff were subject to formal development methods and monitored by auditors for errors throughout their life-history. However, small-scale applications, such as databases developed by end-users themselves, were subject to only ad-hoc monitoring by audit staff. There was anecdotal evidence (but little research evidence) that errors were not only numerous but could be in existence for some time before being detected and corrected. This is recognized in the general auditing literature:

'the correction of errors resulting from serious faults in the introduction of a new or modified system can be extremely costly, and a great deal of damage can be done before correction …' (Coates et al, 1989, p254) [4]

And also by a standard text used for teaching computer auditing in the UK:

'Users of spreadsheet and database packages are necessarily immune from errors. While it is true that such packages provide a safe processing environment within which it is difficult if not impossible to make undetected or obscure input and output errors, it is still possible to make errors in logic. In fact, such errors maybe more difficult to detect than they would have been if a procedural programming language had been employed' (Chambers A.D, 1996, p151) [3]

1.1 Why Errors Occur

It may be assumed that if a novice is well trained in a task then they would make fewer mistakes than otherwise. There is anecdotal evidence, but little research evidence, to suggest that many end-user database builders in companies are either self-taught or taught in-house by non-professional trainers. This poses the 'little learning is a dangerous thing' problem in that such users may consistently overrate their own abilities and thereby make more errors. This is a common problem with novices and is supported by research conducted into comparing self-appraisal and objective tests of learners abilities (Van Vliet *et al* 1993) [1] which indicates that novices of both sexes consistently overrate their own computer literacy skills and hence make more errors. But even professionally trained personnel make mistakes. An assertion made by the authors is that even when training is given it too frequently concentrates on *'how to do things correctly'* and often ignores *'how to avoid doing things incorrectly'*. One possible way of *'avoiding doing things incorrectly'* is to make database builders aware of the common errors they are more likely to make and to encourage them to apply checking controls during development commensurate with the amount of risk associated with producing a possibly incorrect model. This is supported in the auditing literature:

"In terms of teaching …several activities can help students …understand that control should be used sparingly but appropriately; the right amount of control depends on the associated risk" Herremans (1998) [6]

1.2 Types of Errors

Some work has been done on errors in human-computer interaction. Batra and Sein (Batra D.1994) [2] describe work by Norman (1983) which proposed that the human-computer interaction could be represented by:

intention ——> action ———> goal

Norman proposed two types of errors: slips and mistakes. Slips are errors that occur when the intention to act fits the intended goal but the action is not carried out according to plan; mistakes are errors that occur when an action is carried out as intended but the action itself is not appropriate to the task. There is evidence, too, that indicates that novice learners do actually make fewer slips and mistakes after receiving error-awareness training that includes appreciation of the common errors that may occur.

A common problem in teaching is that assessment strategies reward partially correct models whereas in the work-place even one error in a model (depending what it is) may be potentially disastrous. A student, who is happy to be mediocre, when rewarded with a 50% mark for an assignment may be quite pleased with his result and ignore the fact that his model obviously contains several errors. If the pass mark for the assignment is 40% then the student reasons he has 'passed' the task and is therefore competent in it – this is another example of novices over-rating their own abilities (Van Vliet *et al* 1993) [1].

1.3 The Experience of Spreadsheet Errors

Much research has been undertaken on the high incidence of errors in student spreadsheet models from which useful parallels may be drawn for researching the same in database models. Panko R. (2000) [9] cites one experiment in which student spreadsheet developers were given a spreadsheet to build from a written specification. The 'developers' were then asked to estimate the likelihood that they had made an error during development. The median estimate was 10%, and the mean was 18%. In fact, 86% had made an error in their spreadsheet. When debriefed in class and asked to raise their hands if they thought they were among the successful 14%, well over half of all subjects raised their hands. Again, another example of novices over-rating their own abilities.

Work on self-audit approaches to reducing errors in spreadsheet models has shown that increasing the awareness of novices to common errors does make a contribution to improving the integrity of resultant models Chadwick & Sue (2000) [7]. Also, work undertaken by Rajalingham *et al* (1998) [8] has shown that a clear classification of spreadsheet errors may also aid students in improving the integrity of their spreadsheet models.

2. DATABASE BUILDING SKILLS

The work of Chadwick *et al* (1997) [5] and Rajalingham et al (1998) [8] on reducing student errors in spreadsheet models shows that a useful starting point for analysing errors is to have a broad classification of the *types* of skills required in building a spreadsheet. This same classification has been adopted in the analysis of database skills herein.

The classification encompasses four sets of skills. They are Generic and Specific enabling skills and Generic and Specific modelling skills. These sets may serve as a useful starting point for analysing the skills used in database development.

2.1 Database Enabling Skills

Enabling skills are those needed to permit the user full use of the functions and capabilities of database software and may be sub-divided into generic and specific skills.

Generic Enabling Skills are those that give a general understanding of database principles and concepts regardless of the particular product in use.

Examples of generic database enabling skills would be understanding of the concepts of tables, relationships between tables, queries acting upon tables and forms for data presentation.

Specific Enabling Skills are those that enable the user to use their generic enabling skills to manipulate the functions of the specific database software in use i.e. do we fully understand how to use Microsoft Access, Oracle etc?

2.2 Database Modelling Skills

The tables, relationships and queries that constitute the recognised database model are an electronic representation of a business function in the real world. Modelling skills are those required to analyse the business function in order to design the conceptual data model that is to be represented by the electronic database model.

Generic Modelling Skills are those available to a database builder that enable identification of applications appropriate for database modelling (some applications are better modelled with spreadsheets, etc) as well as the skills needed for the data modelling process to occur i.e. entity-relationship diagrams, normalisation, etc.

Specific Modelling Skills are those required to design the specific data model for a given business application. They include data integrity issues such as correctness of table-structure, relationships, referential integrity issues, and SQL that give correctness to a particular model in its real-world business context i.e. does it correctly model the user requirement?

3. IMPROVING AWARENESS USING SEEDED MODELS

In the research conducted herein, students learning database building were encouraged to understand the need for developing error-awareness and the need for self-checking in order to improve the quality of their models. Both of these were accomplished with models, or parts of models containing deliberately induced ("seeded") errors, and then asking the students to identify and comment upon the errors. This approach, of using seeded models, had already been tried and been found to be successful in the teaching of spreadsheet building Chadwick & Sue (2000) [7].

Examples of seeded models used in the teaching approach are given below. Each error shown has been identified from observation of student models by tutors over three years - each year with the final year BSc Hons Computing students.

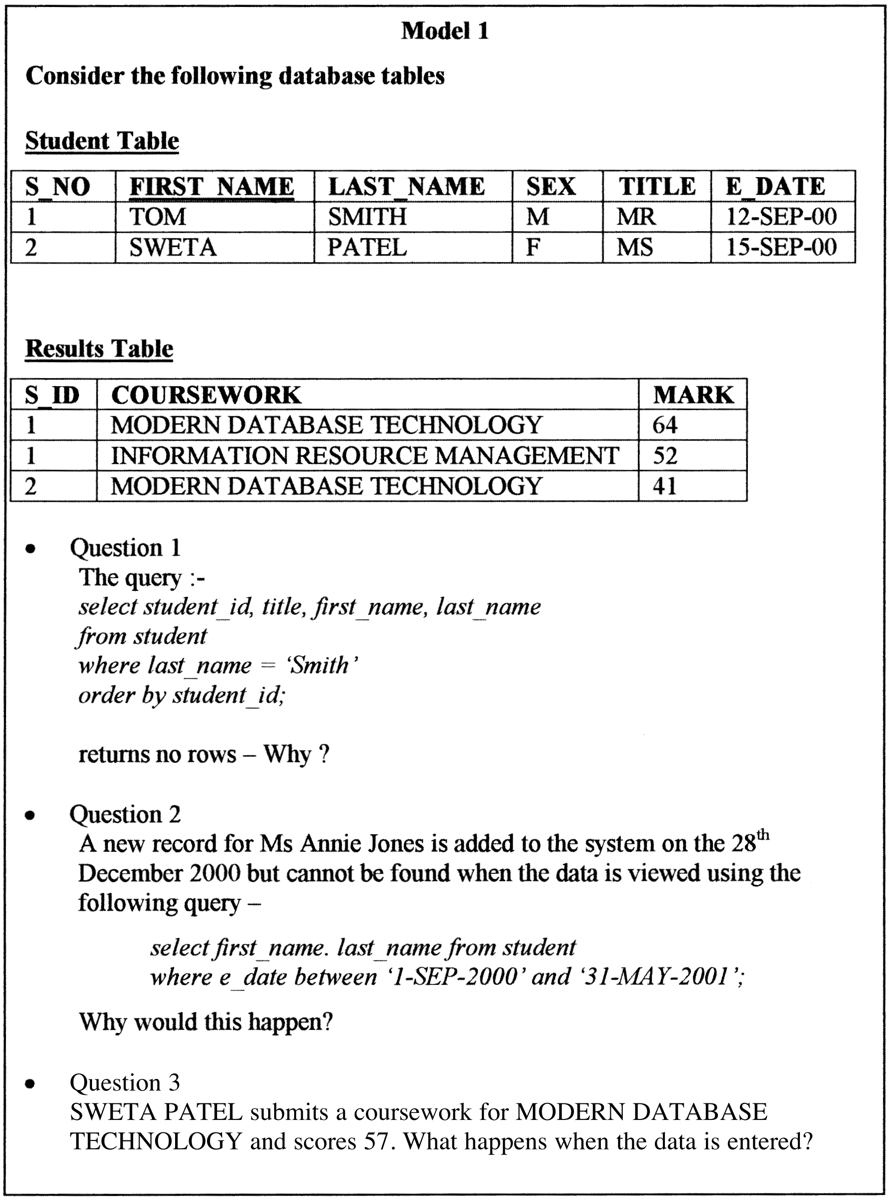
As a matter of interest the reader may like to examine each of the following data models for errors before continuing with the analysis of each model.

3.1 Error Seeded Model 1

Students were presented with two tables containing representative data as shown in **Figure 1** and were presented with a series of questions to consider. The aim of this exercise was to illustrate errors commonly observed by the tutors in both classroom and laboratory situations to raise the students' awareness of these errors.

3.1.1 Analysis of Error Seeded Model 1: Question 1

Question 1 presents a typical query that a student would develop for use with this model, with the experimental result of executing this query, namely that no data is retrieved from the database. The reason for this result is simply that the search string specified in the WHERE clause of the query is in lower case and SQL is case sensitive within single quote marks. Therefore, retrieval of the required records needs to use the WHERE clause *last_name = 'SMITH'* instead. This is an example of generic enabling skills.



Model 1

Consider the following database tables

Student Table

S_NO	FIRST NAME	LAST_NAME	SEX	TITLE	E_DATE
1	TOM	SMITH	M	MR	12-SEP-00
2	SWETA	PATEL	F	MS	15-SEP-00

Results Table

S_ID	COURSEWORK	MARK
1	MODERN DATABASE TECHNOLOGY	64
1	INFORMATION RESOURCE MANAGEMENT	52
2	MODERN DATABASE TECHNOLOGY	41

- Question 1
  The query :-
  select student_id, title, first_name, last_name
  from student
  where last_name = 'Smith'
  order by student_id;

  returns no rows – Why ?

- Question 2
  A new record for Ms Annie Jones is added to the system on the 28th December 2000 but cannot be found when the data is viewed using the following query –

  select first_name. last_name from student
  where e_date between '1-SEP-2000' and '31-MAY-2001';

  Why would this happen?

- Question 3
  SWETA PATEL submits a coursework for MODERN DATABASE TECHNOLOGY and scores 57. What happens when the data is entered?

Figure 1: Error Seeded Model 1 and associated questions

Recognition of this error provides the tutor with the opportunity to discuss the syntax of the query as well as the need for database developers to consider what an end user may enter as search criteria and the importance of accounting for any eventuality. This is typical of the approach to teaching error awareness by providing the student with situations that involve *'not getting it wrong'* compared to *'getting it right'*.

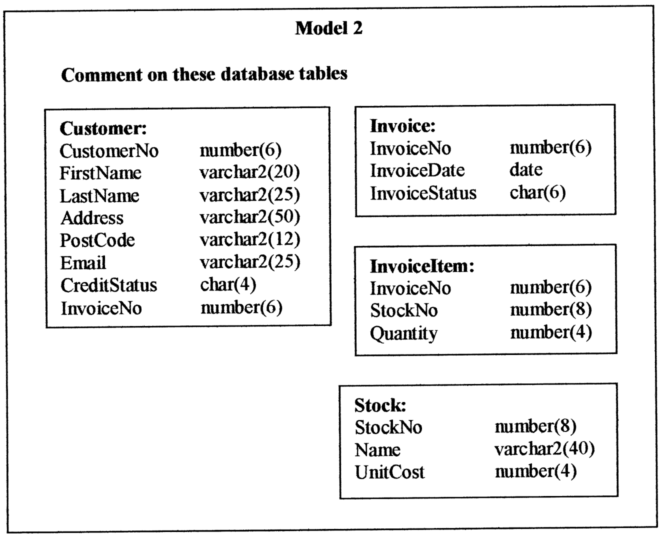
3.1.2 Analysis of Error Seeded Model 1: Question 2

Students were encouraged to consider other potential error situations such as model 2. This question has been designed to encourage the student to consider errors concerned with date formatting. Here a record apparently disappears from the system because data entry of the *e_date* field must have been of the form 'DD-MON-YY', i.e. '28-DEC-00' and recorded as 28th December, 1900. This can be considered as one of the Year 2000 problems and may be due to a number of specific causes.

For example, the data may have been generated from a function that returned the date of the client workstation using a two digit year format although the database required a four digit date format and interpreted '00' as '1900'. Alternatively, the end user may have entered the date and was unaware that a four digit year format was needed. In this way, the student is encouraged to think about the external considerations that may affect their database development and compromise the integrity of the data in their database as well as the potential for error generation by both the system and the user. An example of specific modelling skills.

In the last problem, the student is required to consider what may happen on entry of a potentially duplicate record. Here there are a number of possible outcomes that depend on how the underlying database has been constructed. For example, if a primary key (or unique constraint) has been specified (this would consist of the S_ID and COURSEWORK fields) then an error message should be received indicating that the constraint has been violated and insert of the record is disallowed. However, if this constraint is not specified then the insertion of the record would be allowed which would have repercussions in other parts of the system when two records would be retrieved for the student's coursework grade instead of the anticipated single record. This again provides an opportunity for discussion about the need to protect the database from poor data entry and to discuss possible solutions and strategies for preventing the entry of data that contravenes the business rules of the system.

Error seeded models 2 and 3 are similar problems involving primary key constraints that have frequently been observed in students' work.



Model 2

Comment on these database tables

Customer:	
CustomerNo	number(6)
FirstName	varchar2(20)
LastName	varchar2(25)
Address	varchar2(50)
PostCode	varchar2(12)
Email	varchar2(25)
CreditStatus	char(4)
InvoiceNo	number(6)

Invoice:	
InvoiceNo	number(6)
InvoiceDate	date
InvoiceStatus	char(6)

InvoiceItem:	
InvoiceNo	number(6)
StockNo	number(8)
Quantity	number(4)

Stock:	
StockNo	number(8)
Name	varchar2(40)
UnitCost	number(4)

Figure 2: Error Seeded Model 2

3.2 Error Seeded Model 2

Error seeded model 2 **(Figure 2)** requires the student to detect the incorrect implementation of the relationship between the tables. We have commonly observed that implementation of the 1 : many relationship between tables by posting the primary key of the 'one side' as a field on the 'many side' is reversed with the primary key of the table on the 'many side' posted to the table on the 'one side'.

3.2.1 Analysis of Error Seeded Model 2

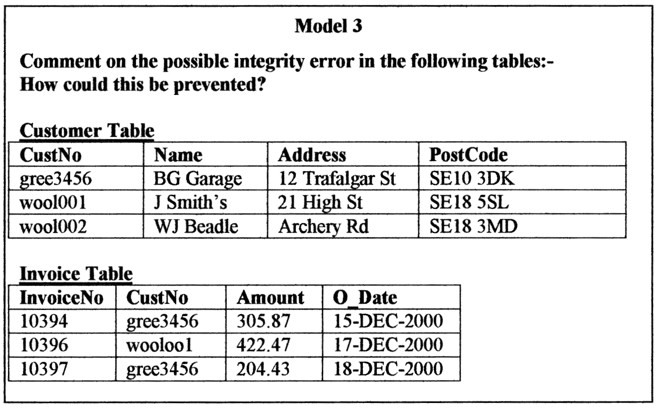
In this example, students should detect the error and identify that the solution is to remove the *InvoiceNo* column from the **Customer** table and implement the relationship by adding a *CustomerNo* column to the **Invoice** table. This should alert the student to the possibility that such an error is common and that they should be careful to ensure that the relationship is implemented correctly. This is an example of a specific modelling skill.

3.3 Error Seeded Model 3

The third model presents two tables and sugest that there may be an error somewhere.

3.3.1 Analysis of Error Seeded Model 3

In error seeded model 3 **(Figure 3),** the error in the data of the tables here revolves around the primary key of the **Customer** table, *wool001*. The related record in the **Invoice** table has as the foreign key, *wooloo1*, where the zero characters have been replaced with the lower case letter 'o'. This could be due to a simple typing error or by reading the value of the primary key in error, typically as the student types in data during building of their system. Naturally, the problem could be prevented entirely by a number of means: for example, correct specification of the foreign key constraint of the **Invoice** table would prevent entry of the incorrect value into the table. However, this example also provides an opportunity to discuss the importance of error protection from the end user by validation of the data on the interface. This may include potential solutions. For example, the use of a format mask on the data entry component of the form to enforce a particular format or perhaps the use of a form element or control that populates the field with the value of the foreign key when the user selects an appropriate customer name.



Model 3

Comment on the possible integrity error in the following tables:-
How could this be prevented?

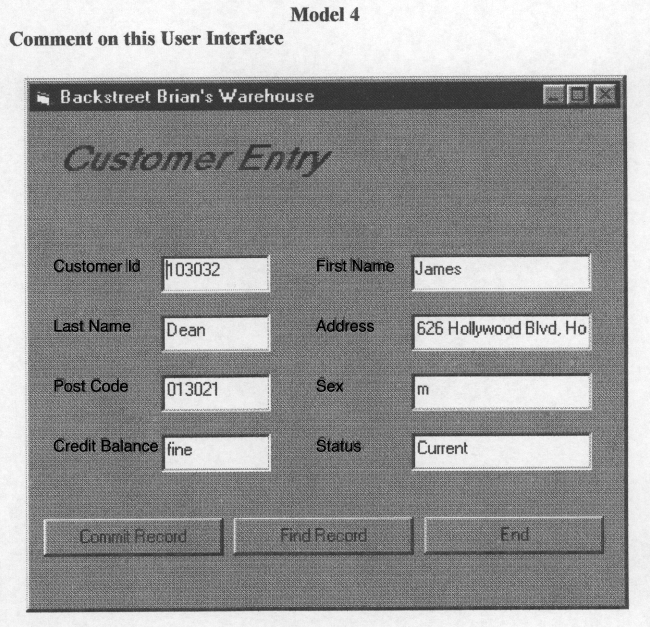
Customer Table

CustNo	Name	Address	PostCode
gree3456	BG Garage	12 Trafalgar St	SE10 3DK
wool001	J Smith's	21 High St	SE18 5SL
wool002	WJ Beadle	Archery Rd	SE18 3MD

Invoice Table

InvoiceNo	CustNo	Amount	O_Date
10394	gree3456	305.87	15-DEC-2000
10396	wooloo1	422.47	17-DEC-2000
10397	gree3456	204.43	18-DEC-2000

Figure 3: Error Seeded Model 3



Model 4
Comment on this User Interface

Backstreet Brian's Warehouse

Customer Entry

Customer Id: 103032
First Name: James
Last Name: Dean
Address: 626 Hollywood Blvd, Ho
Post Code: 013021
Sex: m
Credit Balance: fine
Status: Current

Figure 4: Example User Interface

3.4 Model 4 : Example Of User Interface

Further discussion about the development of a user interface may use the example interface shown in Figure 4. This could facilitate discussion about a number of other aspects of interface development. For example, one could discuss whether the *CustomerId* field should be displayed on the interface or whether it should be concealed, that is, is it a piece of 'real' data (ie does it have significance to the end user). If it has been artificially added to identify the record and only has meaning in the database, the student needs to consider if it needs to be visible to the end user. The Sex field could be used to discuss the importance of making data entry consistent, for example should the user be able to enter 'm', 'M', 'male', 'MALE' or 'Male' for male customers or should the user be restricted to one of these forms. From here the discussion can be pursued by discussing options such as if the user can enter gender in a number of different ways, should the data entered be converted to a standard format before entry into the table. Is there a better way to control data input? Perhaps a set of radio buttons could be used to allow the user to hold the data without the need for typing the data into the form. Similar discussions could involve the contents of the Credit Balance field, and whether it would be better to store the balance as a number, or are there better terms to describe the state of the customer's credit and are there other options for displaying the possible data values?

Students may also comment on the meaning of 'Commit Record' on the button that completes the addition of the record to the database and may decide that there is a better caption such as 'Add Record' or 'Add New Customer Details' or something similar.

In addition, discussion of the interface may turn to whether the layout of the form is acceptable, is it easy to use and does it have all the functions required by the end user and are the colours of the form acceptable and easy to view perhaps all day? This should provide students with a greater awareness of the options that are available for interface development and how these can be used to reduce the opportunities for errors to be made when using the system. This is an example of a specific modelling skill relating to a particular application.

4.0 CONCLUSION

The error seeded models discussed above, as well as others not reported here, were used in conjunction with lecture material on quality issues and software audit to final year BSc Computing students. These students were selected for this project because they have developed skills in both database development and interface design and are required to develop the evaluative skills that form the basis of this work.

Feedback in the form of discussion was obtained from both the full time and part time groups, totaling approximately 100 students. These students had the opportunity of examining the models before discussion of the problems in a classroom setting. All reported that they had enjoyed looking at the models and had learned from it. In particular, they noted that they had started to develop an appreciation for the problems that might be encountered in database development. Some students pointed out that even though some of the errors were known to them because they had occurred during the building of their own databases, the exercise had helped them to appreciate both the extent of the effect of such errors and the options available for avoiding errors.

In developing this strategy, the key factors for the success are:

- early explanation of the rationale for error detection,
- presentation of the models and elucidation of the errors,
- encouragement of the students to think about possible ways to prevent the errors and not simply a statement of the problem,
- monitoring of the exercise by the tutor through guiding the discussion,
- provision of an opportunity for students to exercise and develop their critical judgement.

Further work will be conducted on extending the use of peer and self assessment methods to databases similar to the experiments conducted with spreadsheet modelling and reported in Chadwick & Sue (2000) [7]. Further work also needs to include research into a taxonomy of types of errors and their relative frequencies during the teaching process. The methods used will be refined to produce quantitative results that hopefully will support these preliminary qualitative findings.

5. REFERENCES

[1] Van Vliet P., Kletke M.G and Chakraborty G. *The Measurement of Computer Literacy*. International Journal of Human-Computer Studies Vol 40 , p835-857 (1994)

[2] Batra D. & Sein M.K (1994) *Improving Conceptual database design through feedback*. International Journal of Human-Computer Studies Vol 40 , p, 653-676

[3] Chambers A.D and Court J.M (1994) *Computer Auditing* 3rd Edition. Pitman.

[4] Coates J, Rickwood C.,Stacey R. (1989) *Control and Audit in Management Accounting*. Heinemann Professional Publishing.

[5]. Chadwick D, Knight J, Clipsham P. *Information Integrity In End-user Systems*. Chapman & Hall (Proceedings of the First Annual IFIP TC-11 Working Group 11.5 Working Conference on Integrity and Internal Control in Information Systems, Zurich, Switzerland 3-4 December 1997)

[6] Herremans I.M *How To Turn Students On To The Idea of Control*. Institute of Internal Auditors. 'Internal Auditing' magazine August 1998

[7] Chadwick D, Sue R. *An Approach To The Teaching Of Spreadsheets Using Peer Assessment And Self-Assessment Methods For Reducing Errors*, British Computer Society, (Proceedings of the Fifth Inspire Conference, London, UK, September 2000)

[8] Rajalingham K, Chadwick D. *Integrity Control of Spreadsheets: Organisation & Tools*. Kluwer Academic Publishers, 1998, pp 147-168 (Proceedings of the Second Annual IFIP TC-11 Working Group 11.5 Working Conference on Integrity and Internal Control in Information Systems, Virginia, USA, 19-20 November (1998)

[9] Panko R. Spreadsheet Errors: *What We Know. What We Think We Can Do,* Proceedings of the First Symposium of the European Spreadsheet Risks Interest Group, Greenwich, UK, 2000

The treatment of organisational issues in systems development projects: Bridging the technical - organisational divide

Neil Doherty and Malcolm King

(The Business School, Loughborough University,
Loughborough, LE11 3TU)

Abstract: *Whilst systems development remains a largely technically oriented process, there is growing evidence that it is the effective consideration of organisational, rather than technical, issues that is the key contributor to systems success. However, there is still a high level of uncertainty about the exact meaning, nature and importance of organisational issues. The aim therefore of the research, presented in this paper, was to help clarify the situation by providing an explicit definition and comprehensive register of organisational, combined with an assessment of their relative importance. The research, which was based upon a comprehensive review of the literature combined with a survey of BCS members, provides many pertinent insights into the nature and importance of organisational issues.*

Introduction

Concerns about the quality of computer-based information systems has come to the fore in the last decade, with the publication of reports into a spate of high profile systems failure, such as Taurus, the London Ambulance Service system, the Benefits Payment Card project and the Immigration Service's computer system. However, the statistics suggest that it is not just high profile and complex public sector projects that are predisposed to failure. For example: Hochstrasser & Griffiths [1991 suggest that up to 70% of IS project fail, and an extensive review of systems development practices by Clegg *et al* [1997] found that:

> *up to 90% of all IT projects fail to meet their goals; 80% are late and over-budget and 40% are abandoned.*

Concerns with the quality of information systems should therefore be at the top of all IT managers' agendas.

Typically, discussions of systems quality focus upon a range of largely technical issues, for example, the system's reliability, functionality, response times, accuracy and clarity. Whilst these issues are undoubtedly important, they cannot be said to represent a complete set of quality concerns, as they ignore a wider set of organisational, economic and human factors. A system that is of the highest technical quality cannot be said to be *'fit for purpose'* if it is not well suited to its organisational context. For example, if one takes the case of a major ERP implementation, it will have a massive impact on the organisation, not only in terms of performance, but also in terms of the organisation's design. More specifically, the implementation of an ERP system is likely to modify the organisation's culture and structure, necessitate the re-design of business process, individual tasks and job descriptions, engender changes in the behaviour and attitudes of individual employees, and the alter the distribution of power. If these organisational issues are addressed proactively and explicitly as an integral part of the development project, then it is likely that the technical - organisational fit will be close and the system will be a success, if not, it is likely to result in failure [Doherty & King, 1998]. Unfortunately, whilst there is a growing recognition that the effective treatment of organisational issues is critical to the successful outcome of system development projects, there is little evidence to suggest that they are routinely addressed. This situation has, at least in part, arisen because of a lack of understanding of the true meaning and nature of organisational issues. This overall aim of this paper is to help clarify the situation by presenting the results of a research project that had the following specific objectives:

- To provide an explicit definition of the term *'organisational issues'*, which can be used as the basis for deriving a comprehensive list of specific 'organisational issues'.
- To explore the relative importance of a range of *'organisational issues'*.

Whilst the first objective was explored through review of the literature, and the authors' own experiences of working in this area, the second was tackled through an extensive survey of senior IT executives in UK-based organisations.

Organisational Issues Defined

Typically, organisational issues have been defined by providing examples of *'non-technical'* aspects of systems development, which might have an impact on the ultimate success or failure of a project [Eason, 1988; Hornby *et al,* 1993]. A careful analysis of these examples leads us to propose the following explicit definition for the term organisational issue, which captures the essence of the cited researchers' work:

> *'Those issues which need to be treated during the system's development process to ensure that the individual human, wider social and economic impacts of the resultant computer-based information system are likely to be desirable.'*

Implicit in the use of the term *'treatment'*, in the above definition, is the notion of '*evaluation'* followed by *'action'*; a development team will have to evaluate a specific impact, prior to initiating appropriate action to ensure that the impact is desirable. Consequently, it might be necessary to modify the system's technical specification, or initiate a programme of organisational change, to ensure that all the system's organisational impacts are ultimately desirable. In essence, the treatment of organisational issues is the mechanism by which the project team should match the capabilities afforded, and the constraints imposed, by the technical system to the requirements and characteristics of an organisation and its individual employees.

Given the definition provided in the previous section, it was immediately possible to classify issues such as: the impact of a system on an organisation's culture, working practices, or performance, and similarly its impact on a user's motivation or performance, as human and organisational issues. A full list of the issues, conforming to the definition, is presented in table 1.

The Relative Importance of a Range of Organisational Issues

The definition and register of organisational issues was used as the basis for creating a survey to explore their relative importance. Once the questionnaire had been rigorously tested, to ensure its validity, it was targeted at senior IS executives, who were identified from an appropriate sub-set of the British Computer Society's (BCS) membership list. The survey was ultimately distributed to 3500 executives in UK-based organisations, and resulted in the collection of nearly 600 valid responses, representing a response rate of 17%.

Each respondent was invited to rank the full list of fifteen organisational issues, in terms of their relative importance in determining the successful outcome of systems development projects. These ranks were averaged and are shown in table 2, in ascending order of the mean value. The overriding importance of ensuring a cost benefit analysis in senior IT managers' perceptions stands out. Other issues relating to the system's business contribution, such as 'future needs of the organisation' and 'IS strategy alignment', also appear to be generally perceived as being of importance. By contrast, issues concerned with health and safety and the distribution of power also stand out as being very definitely least important in the eyes of senior IT managers. This is perhaps a rather surprising result given more general concerns for health and safety and the political consequences of any perturbation to the existing distribution of power. The issues inhabiting the centre of the table, which are perceived as being of middling importance, tend to be concerned with the system's impact on individual employees.

It is perhaps understandable that the issues focusing upon the system's contribution to an organisation's performance are generally perceived to be of greater importance than the other issues. However, there is growing evidence that such contributions will only be realised if the necessary organisational change is initiated so that the system can perform effectively. The reasons for this are twofold. Firstly, unless the behavioural and organisational impacts of a new system are carefully evaluated and actively managed the system may not fully realise its full potential due to the likelihood of user resistance [Martinsons & Chong, 1999]. Secondly, information technology is unlikely to deliver significant benefits unless an information systems development project is used as an explicit catalyst for organisational change and process improvement [Ahn & Skudlark, 1997]. The message is therefore clear, systems will only deliver improvements to organisational performance, if an appropriate change management programme, addressing a wide range of organisational issues, is initiated.

Table 1: A comprehensive register of organisational issues.

Issue	Definition
Cost-benefit Analysis	An explicit analysis of the projected benefits of a new system, to ensure that it will meet important organisational needs, within acceptable costs and time-scales.
Information Systems Strategy	A review of the proposed system to ensure that it conforms to the current information systems strategy.
Prioritisation	The allocation of priorities to different aspects of the work, so that the development effort is primarily focused on those areas that are the most organisationally important.
Future needs of organisation	An assessment of how flexible a new system will need to be in order to support other planned or anticipated changes within the organisation.
Process re-engineering	The re-engineering of business processes in conjunction with the development of new systems.
Training provision	The assessment of training needs and the provision of a comprehensive training programme.
Health & safety / ergonomic factors	An assessment of how health and safety / ergonomic factors will impact upon the design of the proposed system.
User motivation / needs	The evaluation of how the motivations and needs of the users will be satisfied by the proposed system.
User working styles / IT skills	An assessment of the users' working styles and IT skills to determine what implications these may have for the design of the system, and the provision of training.
Job redesign	An assessment of whether the proposed system will modify the way in which people undertake their responsibilities.
Timing of implementation	The evaluation of how the timing of the implementation of a new system will interact with the timing of other planned changes within the organisation.
Organisational disruption	An assessment of how much organisational disruption the implementation of a new system will cause.
Organisational structure	An assessment of whether a proposed system will have an impact on the organisational structure.
Organisational culture	The consideration of whether a proposed system is attuned to the culture of the organisation.
Organisational power	A review of how a new system will alter the distribution of power within the organisation, and in so doing anticipate its likely political implications.

Table 2: Relative Importance of Specific Organisational Issues

Rank Order	Organisational Issue	Mean
1	Cost-benefit Analysis	5.39
2	Future needs of the Organisation	6.07
3	Process Re-engineering	6.33
4	Prioritisation of Objectives	6.49
5	IS Strategy Alignment	6.84
6	User Motivation	7.13
7	Timing of Implementation	7.26
8	Training Provision	7.38
9	Organisational Disruption	7.89
10	Organisational Structure	8.21
11	User Working Styles	8.26
12	Job redesign	8.61
13	Organisational Culture	8.74
14	Health & Safety Issues	11.30
15	Distribution of Power	11.45

Conclusions

The research presented in this paper addresses an increasingly important subject, namely the importance and treatment of organisational issues in systems development projects. The research is of importance from an academic perspective in that it is one of the few large-scale, empirical studies in this area, and provides a number of important contributions to our understanding of this research domain. In addition to their academic interest, the results of this study should be of interest or practising information systems managers as they highlight the importance of treating a wide range of organisational issues, rather than focusing on the system's potential contribution. Furthermore, this study may also be of interest, as it provides a clear framework for identifying the issues that need to be addressed in a typical information systems development project. Finally, the paper reinforces the message that the overall quality of information systems must be defined in organisational, as well as technical, terms.

References

Ahn, J. & Skudlark, A (1997) *"Resolving conflict of interests in the process of an information system implementation for advanced telecommunication services"*, Journal of Information Technology, Vol. 12, pp. 3-13.

Clegg, C., Axtell, C., Damadoran, L., Farbey, B., Hull, R., Lloyd-Jones, R., Nicholls, J. Sell,R. & Tomlinson, C. (1997) *"Information Technology: a study of performance and the role of human and organisational factors"*, Ergonomics, Vol. 40 No. 9, pp. 851-871.

Doherty, N. F. & King, M. (1998) *'The Consideration of Organisational Issues in Systems Development Projects'*, Behaviour and Information Technology.

Eason, K., (1988), *Information Technology and Organisational Change,* Taylor & Francis, London.

Hochstrasser, B. & Griffiths, C. (1991) *Controlling IT Investment,* Chapman Hall, London.

Hornby, C., Clegg, C., Robson, J., McClaren, C., Richardson, S. & O'Brien, P. (1992) *"Human & Organisational Issues in Information Systems Development"*, Behaviour & Information Technology, Vol. 11 No. 3, pp. 160-174.

Martinsons, M. & Chong, P. (1999) *"The influence of human factors and specialist involvement on informations systems success"*, Human Relations, Vol. 52, No. 1, pp 123-152.

End note: *The authors are about to embark upon a series of interviews with IT professionals, to explore how organisational issues can best be treated in practice. If anyone would like to participate in this study, could they please contact Neil Doherty on 01509 223128, or n.f.doherty@lboro.ac.uk,*

Neil Doherty *gained his PhD in software engineering from the University of Bradford. He is currently a Senior Lecturer in Information Systems in the Business School, at Loughborough University. His research interests include: the treatment of organisational issues in systems development projects; success and failure in systems development projects and strategic information systems planning.*

Malcolm King *is the Professor of Management Sciences in the Business School, at Loughborough University. As well as Mathematical modelling, his research interests include the impact of IT on all areas of management and the organisational and political aspects of systems development. He has also written on the acceptance of IT and its application within small and medium-sized enterprises.*

An Analysis of BS7799 and Requirements for ECommerce

Gary Gaskell

Bank of Queensland, Australia

gary.caskell@boq.com.au

ABSTRACT

There are increased calls for the assurance of information security as society becomes increasingly dependent upon information technology. The escalating attacks on computer networks is due to the dramatically increasing large-scale interconnection of every organisation to every other organisation.

On top of this situation there is rapid deployment of commerce over this interconnection of systems, known as electronic commerce (ecommerce). In this environment there are calls for security standards. The oft cited "industry best practice" is in reality - not defined at all and hence there is a strong need for the clear definition of security requirements. The recently revamped BS7799 is an attempt to fill the void. This standard is now proposed to become an ISO standard for IT security management. This paper examines the appropriateness of BS7799 for providing assurance of information security in the electronic commerce context.

This paper argues that BS7799 provides insufficient security for ecommerce. It is, however, acknowledged that by proper application of the threat/vulnerability/risk assessment process that adequate security can be obtained. The overall framework provided by BS7799 is also very worthwhile. The BS7799 is not a standard that can be directly applied for ecommerce security - so proceed with caution!

Keywords

Information Security, Electronic Commerce, BS7799, standards, security requirements.

1. INTRODUCTION

The correct operation of computing systems is notoriously difficult to verify. This is a well known fact dating back to the classic articulation by Dikjstra. It is also true in the field of IT security. In general the IT industry attempts to address this by defining a standard and then assessing the level of compliance to that standard. There are many standards concerning different aspects of IT security. Furthermore there are various recommendations published by organisations such as the National Institute of Science and Technology (NIST), the United States Department of Defence (US-DOD), the Carnegie Mellon University based Computer Emergency Response Team (CERT), the Internet Engineering Task Force (IETF) and the United States National Security Agency (NSA).

The British Standards Institute of the UK has its own standard known as BS7799:1999 (Information Security Management). The primary objective of this article is to assess the BS7799 standard for its adequacy for defining the security requirements for electronic commerce (ecommerce) deployments.

2. ECOMMERCE SECURITY REQUIREMENTS

The large scale integration of networks via the Internet is permitting the rapid deployment of ecommerce. There are many reports[1] of the huge potential for growth in this sector of the IT industry. There is also an increasing potential for security breaches. Many organisations have connections direct to suppliers or service providers in addition to their Internet connection. It is not uncommon for an organisation to have in the order of 10-20 such connections[2]. Each of these organisations is also networked to other parties - who are often competitors of the service provider's clients. It can be seen that any particular organisation has multiple external connections. This is dramatically different from just five (5) years ago when it was only typical to have dia-in support from a small number of support providers.

This increased opportunity for attack on an organisation's core systems leads to requirements for increased robustness and breadth of the security systems in place.

There are three parts of a threat assessment - assets, agents and opportunities/methods. In ecommerce systems the agent may be financially motivated competitors or ciminals, hacktivists, vandals or benevolent hackers. The wholesale interconnection of almost every organisation via the Internet opens up an enormous opportunity for attacks. Further, the potential for attacks to not be addressed by law enforcement authorities due to jurisdictional, lack of evidence or lack of expertise is a large concern.

In the realm of ecommerce it can be seen that the largest threat comes from external sources. The classic view of IT security was that 80% of the threat was due to internal personnel. As the major threat is from external sources, it is not within the organisation's

* This paper was prepared while the author worked at the Information Security Research Centre and the Queensland University of Technology. Much credit must be given to Professors Dawson, Longley & Caelli for creating an excellent centre within which to study and to conduct research.

[1] These reports are commonly found in newspapers and from Information Technology industry research companies such as Gartner and IDC.

[2] This assessment is based upon experiences gained from network security audits.

ability to influence the behaviour of these external sources. Hence personnel vetting and operating procedures cannot dramatically reduce the risk to the organisation. The best that ecommerce systems can do is to install technical countermeasures, particularly where the countermeasures are on a server controlled by the organisation. In an ideal situation an organisation does not rely on the use of technical mechanisms deployed on systems operated by clients/customers. For example it is unrealistic to rely upon the security of a user's personal computer in the business to consumer ecommerce scenario.

Best practice is often used for security reviews due to the lack of acceptable standards. A best practice security review for ecommerce sites should specifically seek to answer the following questions:

1. Is there a security policy that defines the required protection of assets - not the controls?
2. Are all know and exploitable vulnerabilities fixed (i.e., are vendor patches up to date and all unnecessary network services disabled)?
3. Is the accountability strong (i.e., is user authentication strong enough and are logs protected)?
4. Is there enough defence in depth for highly exposed machines/services (i.e., the Internet gateway)?

The recently updated BS7799 is reviewed agains this background.

3. BS7799 ANALYSIS

The British Standard for Information Security Management is BS7799. It is used worldwide (e.g., by Boeing and ISS[7]) and has recently been adopted verbatim in Australia as AS/NZS4444. Further, it has been submitted to ISO/IEC under the fast track procedure for new international standards. Part 1 has recently been accepted as ISO17799:Part 1.

This standard aims to provide "a comprehensive set of controls comprising the best information security practices". Part 1 is effectively a catalogue of security controls. Many of these controls are at the conceptual level rather than at detailed technical level. There are some exceptions such as details on passwords. Part 2 of the standard presents a base-line of control measures selected from Part 1. The author intends to show that the set of controls is not comprehensive enough for ecommerce.

Part 1 identifies that this standard is a starting point for developing an organisation's security specification. It also identifies that additional controls may be required. As stated above, the primary objective of this paper is to identify where the listed controls may not be adequate for the deployment of ecommerce.

It is stated up-front that thorough risk assessments and the corresponding security plans will address the concerns raised in this paper. However the standard aims to provide a catalogue of security controls and it is worthwhile to identify the deficiencies of this catalogue with respect to ecommerce deployments particularly as various consultancy and standards bodies are promoting this as an "ecommerce standard". The weaknesses identified are not based on paranoia, but rather on the knowledge[4] of what has broken in the past.

3.1 Discrete Issues Concerning BS7799

Definitions

BS7799 does not define many of the terms it uses. This may seem to be an odd point to criticise as the standard is easy to read. It should be expected that many readers will not be security specialists. Also recent industry experience has shown that people get the definitions wrong[3].

An initial motive for the development of BS7799 was that certfication of good security practices would facilitate the safe interconnection of systems for organisations involved in information sharing arrangements. However, BS7799 does not specify a common standard for all systems, but rather it outlines a framework for information security management. The standard requires that the controls used by an organisation are "appropriate" for that organisation's needs. This does not meet the extension, that, the controls are appropriate for other organisations who may be inter connecting. This is one significant reason that BS7799 is not appropriate for ecommerce security.

The term "appropriate" is not defined. This is a similar problem to defining "secure", as secure is not a binary condition. Secure needs to be defined with respect to the threat (asset value, agent and opportunity/methods). It is not possible to define up front what "appropriate" is in every situation. However, rather than just using the word in its general sense, the standard should provide some guidance as to what is "appropriate". Without such guidance, there is not really a "standard".

An example to illustrate this point might be a bank that permits access by a vendor, where the vendor also has clients who are competitors to the bank. It can be expected that the "appropriate controls" selected by the bank under BS7799 will be very different to the controls selected by the vendor. Another example might be a health service provider and the interconnection with their Internet service provider.

Risk Assessments

BS7799 can be protected from criticism by its reliance on a risk assessment for any situation where the control measures in its catalogue are insufficient. A standard is typically intended to reduce costs by defining the acceptable specifications without resort to expensive analysis. It is noted that industry has responded to this with its own standards which are technically specific. See [1, 6, 9].

Threat Agents

The reading of the whole of BS7799 gives the impression that the main concern is with controls for internal threats. The majority of the controls are aimed at reducing the threats from internal users and application faults. The standard does not directly address the threat posed by crackers[4].

Misunderstanding of BS7799

BS7799 is clearly a management (or technical management) standard, but many people expect it to be a detailed technical specification. This is not the fault of BS7799, but nevertheless, this point must be stressed. Two separate systems accredited under BS7799 have no guarantee of providing the same level of security. Hence, two independent applications of the standard can fail a repeatability test. Application of the standard does, however, provide assurance that the management in each organisation have a system in place to provide themselves with "appropriate" protection. Put simply, the difficulty is that the standard requires that a "good job" be done of IT security management, but it fails to articulate how a "good job" is defined.

[3] Some consultants from a world wide consultancy firm recently referred to vulnerabilities as probabilities, when they really meant to state the risk, whereas a vulnerability is simply a weakness.

[4] A cracker is identified separately from a hacker in that a cracker gains illicit system access, often by crafty misuse of network services.

Effectiveness

On page 4 of Part 1 the standard rates the effectiveness of the controls in place according to the number of incidents. This is very inappropriate in the realm of ecommerce. A serious security breach with some ecommerce deployments could so seriously jeopardise the viability of an organisation that the security controls need to be such that no breaches occur. For example, public confidence could be so seriously damaged by a single breach of an ecommerce trader's security, that it could cease to trade. It is not a valid methodology to rate the effectiveness of the trader's security defences according to the number of security breaches. The absence of a breach cannot confer that there is adequate security in place.

A problem in today's IT security systems is that due to the complexity of many computer systems it is difficult to implement controls that do not have imperfections. With this acknowledgement the management of the security must involve techniques such as product evaluation and/or defence in depth designs. BS7799 does not explicitly identify this. The Information Technology Security Evaluation Criteria (ITSEC)[2] contains the concepts of the effectiveness and completeness of controls. The effectiveness is whether the control can be bypassed or thwarted. The completeness concerns whether the whole of the threat is addressed, as there may be several controls used to redress one threat.

These concepts relate to the design and selection of controls and greatly help the assurance received.

BS7799 does not properly and adequately address the issue of effectiveness and completeness of security within a system.

Classification

The classification of information is about deciding priorities for protection. Section 5.2 of BS7799 Part 1 requires a classification system to be in place together with an appropriate access control system. The addition of a default classification scheme would greatly ease the design of an organisation's security. It could be expected that many organisations could use a system that classified all data as internal by default, required explicit authorisation for external disclosure and practiced the "need to know" principle for the more sensitive of an organisation's information. Another advantage of this addition would be a common understanding of data classifications in the IT industry. BS7799 requires that an organisation has a classification system but fails in not providing a default classification scheme. This would greatly assist system security architects.

Evaluation

Section 8.2.2 of the standard (System Acceptance) presents some criteria for the acceptance of new products or systems. The section calls for the testing of the new system to verify that criteria are met. It is well known however that testing can never hope to identify all faults. This is why the Common Criteria standard [8] for security products has many requirements for the development process itself. This section could be enhanced by indentifying the benefit of third party evaluation of a product's security claims and by requiring a sound development process.

Quality of Cryptography

The most important aspect of secure key generation is that the cryptographic keys are unpredictable. This unpredictability requires that the key generation is based on quality random or pseudo-random numbers. The consequences for the security of ecommerce were obvious as far back as 1996 when an exploit based on a vulnerability, due to low quality randomness, was demonstrated[5]. Section 10.3.5.1 of Part 1 of the standard deals with "Key Management". It does not mention randomness in the discussion on key generation. The location, seeding and pseudo random number algorithms are key parts of the cryptographic mechanisms and security of ecommerce.

The key management section severely lacks any serious discussion and guidance concerning key management. This section should either provide detail or refer to other standards that detail the proper security requirements concerning key management. Randomness in key generation is only one issue. There are also several other issues such as key storage, key decay, key distribution, key replacement, key archiving and key strength.

Known Vulnerabilities

The issue of security patches is one of the first inspections on a best practice security audit. Security patches are released by software vendors to fix vulnerabilities. Once a patch is announced by the vendor, there is a public awareness with both the good and bad elements in society that the software in question contains an exploitable weakness. In today's industry the almost daily announcement of new vulnerabilities is quite alarming. For example, Microsoft Corporation[5] has announced 100 vulnerabilities in the year 2000. There is now a culture of disclosure amongst vendors. This allows system owners to know where their systems have security weaknesses. However the disclosure of vulnerabilities is also monitored by potential intruders and this makes it even more essential that security patches are applied in a timely manner.

Experiences from security audits shows that security patches are rarely up to date. This is difficult to explain considering the opportunities for exploitation in the realm of commerce systems. BS7799 does not mention security patches in the Section 4.8 of part 2 on "systems development and maintenance". One of the common questions to us as auditors is, "what time frame is acceptable for the installation of vendor patches?". Of course a risk assessment reponse is one answer.

BS7799 should explicity discuss the management of implementing vendor patches. The timing question is then an assessment of the ease of exploitation and the impact on the organisation.

Malicious Content

Considering the generic approach of much of the BS7799 standard towards vulnerabilities it is perhaps with some surprise that it explicitly mentions "malicious software" (viruses/trojans). However, this whole section misses the concept of "malicious data". Malicious data is the most common way that crackers break into networked systems. CERT[4] has said that 50% of break ins over the last 10 years have been the class of attacks known as "buffer overflow attacks". These vulnerabilities are exploited by a malicious third party sending specially crafted data to a vulnerable machine. Today's best practice Internet gateways deploy realtime intrusion detection engines that aim to identify this malicious data and react if possible.

The broad area of both malicious code and malicious data should be explicity discussed in the standard as it is of direct relevance to ecommerce systems.

[5] Microsoft Corporation is not alone, but perhaps has the most numerous number of security announcements. Linux has also had many security flaws announced in 2000.

System Integrity

Section 8.7.6 of the standard discusses "publicly available systems". It states that systems should be protected for integrity by using appropriate mechanisms. Digital signatures are mentioned. However this is only one of the available mechanisms. While Transport Layer Security (TLS or also known as SSL) may use cryptography (it uses symmetric keyed hash algorithms for content integrity), this does not guarantee the authenticity of a web page document or a database record but only that the document came from the authenticated server. TLS only protects the channel. Other tools such as Tripwire, developed at Purdue University, use cryptographic techniques to detect integrity violations of content stored in file systems on networked servers. This is a common mechanism that is recommended by CERT. Integrity mechanisms should be listed in the catalogue of controls provided by BS7799.

Electronic Commerce

Section 8.7.3 of BS7799 on ecommerce security does not specify any control options. The standard raises 9 questions (sections 8.7.3.a-i). This section does refer the reader to Section 9.4.7 that discusses network access control. Section 9.4.7 lacks detail, although it does state that network access control will be required.

From a standards viewpoint, this gives very little direction as to what standard of network access control is appriopriate. Alternative standards such as the BSI[3] give direction such that the main filtering firewall host should not be subject to direct attack (i.e., use a filtering router to protect it). Another important issue for HTTP based commerce is the session state that is maintained by using HTML cookies. If good cryptographic techniques are not used with cookies, it may be easy for attackers to hijack sessions.

This "light touch" approach to security specification will lead to greatly varying degrees of security obtained by organisations in their ecommerce deployments. It is clear that BS7799 cannot provide assurance to consumers or clients of an ecommerce organisation that the client's data is adequately protected. Neither can it ensure information is protected to a certain level of technical quality. This is another weakness in the standard. The standard should detail the controls required.

Authentication Quality

A major area of concern with BS7799 is its handling of user authentication. Section 9.2.3 of part 1 directly addresses passwords, but passwords are only one form of authentication - albeit a very common one. This appears to derive from the BS7799 implicit focus on internal users, rather than on extranet/ecommerce type of systems. Elsewhere the standard does acknowledge that biometrics and token based systems are available - but that is all it does acknowledge. There are no requirements for the quality or resilience of authentication mechanisms, other than "risk assessment".

Under this approach a risk assessment needs to justify why plaintext passwords are not secure enough when travelling on untrusted networks such as the Internet. The password sections of this standard also focus on relying on the user for password characteristics (section 9.3.1).

It is inappropriate for user authentication standards to be the same as for the authentication of privileged users such as system administrators. For example, it is common industry practice that superuser passwords on Internet accessble servers are just random characters. BS7799 also permits reuse of passwords on different systems. This is not acceptable on key ecommerce systems. The standard also permits six (6) character passwords. However it is common in various industries to use eight (8) characters. It is also considered best practice to use the full 14 characters for the administrative accounts on Windows NT servers. In general these password suggestions by BS7799 are not good enough for ecommerce.

Logs and Accountability

Section 8.4.1 of part 1 discusses backup. Best practice in the security field states that full system backups are performed prior to deployment. Also best practice ensures that logs are backed up. The standard does not list these controls.

The maintenance of records is mentioned in several places in the standard. Best practice in industry says that logs should not be stored on the machine that they are trying to protect. It is well known that crackers quickly remove traces of their illicit entry from the system logs. The control for this is to send logs to a remote secured log server in realtime. This is relatively easy for Unix servers, but requires additional commercial software for Windows NT servers. BS7799 does not identify these controls. Neither section 9.7.1 on event logging nor section 4.7.7 in Part 2 discuss log integrity.

BS7799 poorly deals with event logging and in particular the maintenance of the integrity of such logs.

Policies

The writing of security policies is often considered to be hard. At least, many network managers treat the issue with dread. The standard gives very little guidance in this area. The natural way to approach a difficult and complex task is decomposition. One approach to decomposition is to separate the policies that specify what is to be achieved from the policy of how it is to be achieved. Consulting experience in industry shows that some organisations call a set of firewall rules their Internet policy. Obviously this is not something senior management of an organisation can sign off on and if they do sign off on it, then they are exposing themselves to personal liability if there arises a security breach. Other organisations write security policies based on generic requirements and then hand these policies to a contractor as the policy that is to drive the fireall configuration.

Obviously both of these approaches to policy design are flawed. Security is critical in ecommerce as it has a direct relationship to the level of trust that can be bestowed upon the system.

BS7799 would be greatly enhanced if it provided practical guidance to the structuring of security policies.

Miscellaneous

A simple requirement of "best practice" audits by industry requires that organisations remain abreast of all known vulnerabilities. A common way to meet this objective is to join CERT or AusCERT (The Australian CERT) [4]. This would be a good addition to the standard.

It is common practice in government and defence software projects to require the developers to identify all know construction vulnerabilities. This allows the issue to be managed. Section 10, systems development and maintenance, of BS7799 does not list the identification of vulnerabilities as a control mechanism.

4. CONCLUSIONS

BS7799 is a standard for the management of security and has as its main focus internal threats to information assets. Ecommerce is largely open to threats from external sources and, therefore, the control measures contained in BS7799 are insufficient for electronic commerce deployment. This paper has outlined multiple instances of situations where additional controls would be required to meet the so called, “industry best practice”.

Despite these shortcomings, BS7799 is a good starting point for managing IT security. BS7799 sets out controls which represent the minimum baseline for internal security but it is not sufficient for Internet connected ecommerce solutions.

The most important shortcomings which require addressing before BS7799 could be relied upon as a sufficient security yardstick are vulnerability management, system integrity, authentication quality and logs and accountability.

5. REFERENCES

[1] http://www/truste.com

[2] *European Community advisory group Seniors Officals Group Information Systems Security*. Information Technology Security Evaluation Criteria. Department of Trade and Industry - United Kingdom, June 1991. Version 1.2.

[3] BSI. German IT Security Standards. http://www.cert.org/

[4] CERT. CERT Coordination Center. http://www/cert.org/

[5] G Gaskell and B Broom. *On The Recent Attacks Against WWW Systems*. In T Bossomaier an L Chubb, editors, Proceedings of Australian Unix and Open Systems Group Conference, pages 28-36, September 1996. ISMN 1-975781-71-4.

[6] ICSA. TruSecure. http://www.icsa.net

[7] ISS. http://www.iss.net/

[8] Common Criteria Project. *Information Security Evaluation Common Criteria*. International Standards Organisation, 1998. ISO 15408 (Common Criteria Version 2).

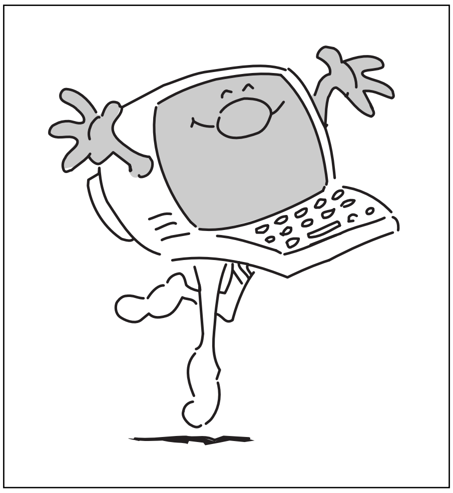
[9] Steve Sutton. *Windows nt security guidelines*. Technical report, Trusted Systems Services, June 1999. http://www/trustedsystems.com

Acknowledgements

Acknowledgements must be given to two esteemed gentlemen in the security industry for their advice and support in writing this paper. Firstly Adrian McCullagh (of Gadens Lawyers and soon to be legal counsel for Spyrus USA) gave extensive comments and provided lively discussions. Svein Knapskog (formerly of the Norwegian University of Science and Technology - Trondheim where he helped guide ISO15408 through ISO/IEC and now with uninett.no) has been a mentor for me in the IT security field.

HUMOUR CORNER

Caption Competition



The most amusing and original caption received by the editor at the email address on page 3 by 31st August will win a prize.

The Web Page

Looking for a Smart Move

Andrew Hawker

University of Birmingham

The Smart Card has long been heralded as the next big step forward in security and control, particularly in financial transactions. Nevertheless, in the real world users have taken a rather cautious approach, and progress has generally been slow and patchy. This can partly be attributed to the costs and logistics involved, but there are also some more strategic concerns. For example, companies fear that by jumping on the wrong bandwagon, they may end up with a standard which fails to catch on. By their nature, many smart card applications need to operate across many different systems, perhaps located in entirely separate organisations. No-one wants to adopt a standard which will be out of step with others in their industry. There may also be anxieties about the ability of a particular card or standard to cope with requirements in the future.

In theory, these are all questions which should be easy to research on the Internet. It should be possible to track down the authors and supporters of the various standards, and to find out which of them have actually been used in trials. Above all, the Internet should be able to give the very latest and most up-to-date picture.

As ever, life is not quite that simple. This column describes a number of sites that can provide useful information. Given the huge number of sites that discuss smart cards in one way or another, it makes no claim to be comprehensive.

In the United States, two of the main industry organisations have recently merged. The Smart Card Industry Association and the Smart Card Forum have joined forces to become the Smart Card Alliance. The Alliance has a site at **www.smartcardalliance.org**. The "Knowledge Base" at this site has a good collection of articles, including some in a "Security" section, and lists details of the main standards which apply to smart cards. Much of this is available for anyone to browse, although some material is restricted to subscribers only.

A much smaller site is provided by Card Europe, another industry association. This can be found at **www.cardeurope.demon.co.uk**, and offers very little in the way of information for the general browser. The European ePayment Systems Observatory, on the other hand, provides a good bibliography of articles relating to all aspects of smart card implementations, at **epso.jrc.es/purses.html**.

For those interested in financial applications, three sites can be recommended, all of them part of the Mastercard virtual empire. Probably the best known of these is at **www.mondex.com**. This tries to cater for a number of different audiences, and so there are some simple explanations of the principles of the Mondex card, aimed at the general public, alongside the kind of technical and commercial information that is more likely to interest business clients. The design is tight and simple, and avoids the gimmicks and longwindedness to be found on many web sites. However, this brevity can be a bit frustrating at times, as can some of the signposting : (for example, "How Mondex works" takes you to a description of the Mondex organisation, not the technology). There are numerous descriptions of Mondex projects, classified by location, and a brief overview of the system's security features. There are not many pointers to other sites, and trying to follow one of them, to the Open Trading Protocol, lands you on the home page of the Mastercard main site. Various searches for OTP from this point on proved fruitless. Information on the OTP protocol is probably best found from the "horse's mouth", at the Internet Engineering Task Force site at **ftp.ietf.cnri.reston.va.us** (look under the heading of "trade").

The two other sites with the Mastercard connection are **www.multos.com** and **www.interactiveloyalty.com**. The former of these promotes the MULTOS "open, high-security, multi-application operating system" for smart cards. This site lists the companies involved in the Consortium promoting MULTOS, and features a number of case studies, predominantly in the banking sector. Interactive Loyalty, on the other hand, promotes "the next generation of loyalty cards". Again this features an impressive list of business partners, and tries to be of interest to a broad spectrum of readers. The next generation of loyalty cards, in case you were unaware, will ".. deliver highly targeted, individual and relevant offers to customers, make the most of cross-selling opportunities, help migrate customers to higher margin products, and provide an excellent way of helping to make customers feel special. Interactive Loyalty is also particularly suited to strategic alliances of organisations that wish to run joint loyalty programmes". If you want some further reading on the kind of multi-function card systems which all this implies, you can download a very readable report (Adobe format) written by staff at the Bristol Business School, which includes a couple of pages on security and fraud issues.

Meanwhile, details of a rival outfit can be found at the Global Platform site (**globalplatform.org**). Here, another association of well-known industry names can be found promoting the set of Open Platform card standards. The technically-minded can download these in full, provided they are willing to enter into a licence agreement (free of charge). The tone of this site is relentlessly businesslike, making little attempt at sweet talk about the commercial benefits of multi-function cards. Anyone wanting to see the selling points of smart cards set out more vigorously should turn to one of the many vendors operating in this marketplace - for example, at **www.activcard.com, www.cardlogix.com** or **www.smartdynamics.com**.

Andrew Hawker can be contacted at the University of Birmingham on 0121 414 6675 or by email A.Hawker@bham.ac.uk

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)

Colin Thompson, BCS Deputy Chief Executive, provides a view from HQ on some of the major current issues for the Society.

THE AGENDA FOR CHANGE

In my column in the last edition of this *Journal*, I outlined the programme for modernising and revitalising the BCS. Things have moved on significantly since that time in each of the three main areas of the programme:

- ◆ The new Brand strategy
- ◆ Improving our Web-based capability
- ◆ The new organisational structure

THE BRAND STRATEGY

The new BCS brand was launched, on schedule, in June and the new logo now appears on all correspondence from BCS HQ and on the BCS web site. New designs, incorporating the logo, for all other material, will be introduced over the course of the coming year.

The design for the logo is based on the key from the Coat of Arms that the Society has used as its identifier since 1984. The use of the crest will continue, but the key will be the primary identifier on all material emanating from the Society, including HQ, Branches and Specialist Groups. With very limited exceptions – such as the ECDL brand – the use of the various other logos, in use across the Society will be discontinued.

The main purpose of this part of the programme is to ensure a consistent look and feel to all our material. One of the main messages from recent surveys has been a lack of understanding of the purpose of the BCS, of what it does and what it stands for. There is a very real need for greater clarity of message and the new branding strategy is part of that. Consistent branding will not solve all the problems of course, but it is considerably easier to present a consistent image and message if all our material appears to come from one family.

One advantage of the new logo over the Coat of Arms, will be an increase in the flexibility of its use. All crests granted by the Crown are subject to very specific restrictions and it has been impossible, for example, for the Society to allow members to use it on their letterheads. The rules for the use of the logo, however, are set entirely by the Society and we will be encouraging members to use it to identify their membership wherever appropriate.

Further information on the new branding can be found on the BCS web site. All the approved designs are available for downloading, with the rules relating to its use.

THE BCS WEB INITIATIVE

The aim with this part of the programme is to put the Web at the centre of our service provision. The web will not replace more traditional means of communication, but the Society recognises that it can only deliver the level of service, communication and engagement needed for the future by exploiting fully the potential of the internet and the Web.

The Society is committed to a major investment programme, not just to improve the information available, but also to link the web site to the various back-office systems so that our major transaction processes can be fully web based from end to end. A contract to undertake the necessary work was signed with Ramasys – the supplier of the software used for the main member database and associated applications –in May, and work on the first phase of the project is now underway. That work is likely to continue for around 18 months, but new facilities such as the ability for members to update their records will appear gradually over that period.

THE NEW ORGANISATIONAL STRUCTURE

As I mentioned in my last column, there is a general recognition that the BCS of tomorrow cannot be created by the organisation of today. A new structure is essential if we are to establish new modes of behaviour and to change from what some regard as a cosy club to an organisation with its roots well established in its member and customer base.

At its meeting in May, Council gave final approval to organisational proposals presented by the Policy and Resources Committee. That decision means that the existing structure of 7 Boards will be replaced, as from the AGM in October this year, by a new structure comprising 4 Boards and 3 Member's Forums, each led by a Vice President. The following list gives a brief summary of the purpose of each of these main elements of the new structure:

Member Services Board Vice-President Charles Hughes

- ◆ To ensure the Society is providing its members and other interested parties with the information and related services necessary for effective professional practice at all levels.

Qualifications and Standards Board Vice-President John Chapman

- ◆ To establish and maintain appropriate standards of education, experience, competence and conduct for information systems practitioners and engineers.
- ◆ To encourage and promote adequate provision of education, training and qualifications to allow practitioners to develop and maintain effective careers
- ◆ To establish and maintain effective arrangements for the accreditation of academic courses, training provision, career development schemes and competence assessment arrangements.
- ◆ To ensure the proper management of the processes by which applicants are admitted to Society membership and affiliation and by which members are nominated for registration with the Engineering Council and FEANI

◆ To provide mechanisms and related quality assurance to review the performance and conduct of members and affiliates in relation to relevant standards

◆ To ensure that appropriate quality assurance and audit arrangements for all processes within its area of responsibility, including those relating to Engineering registration.

Knowledge Services Board
Vice-President Professor Wendy Hall

◆ To develop and disseminate a wide variety of knowledge about IS and its application to the IS professional community, business management and educational establishments.

External Relations Board
Vice-President David Morriss

◆ To establish the Society as the recognised authoritative source of leadership in IS practice and to manage the arrangements for the external representation of the Society. Its constituent audience will be IS practitioners, Government and other bodies concerned with professional IS practice.

Engineering and Technology Forum
Vice-President Professor John McDermid

Management Forum
Vice-President Rachel Burnett

Education and Training Forum
Vice-President not yet appointed

◆ To provide a network within which members with relevant interest, experience and expertise in the areas of information systems engineering and technology, management, and education and training are encouraged to engage with the activities of the Society, exchanging ideas of common interest, influencing the work of the Society and supporting its programmes.

Of the Vice Presidents listed above, four hold VP positions in the current organisation and two, Rachel Burnett and Charles Hughes are new to the role.

The change to be introduced in October signals not just a new organisation to handle the business of the BCS but a new way of handling that business. Boards will be smaller and concerned more with strategic issues; committees will be encouraged to focus on delivery rather than debate. They will be expected to work to a programme of planned deliverables and to account for performance against that plan. Starting from September this year, the Policy and Resources Committee will review reports from each Board and Committee, showing the achievements of the previous year and the activity and deliverables planned for the next two years.

Whither the Specialist Groups?

One of the Boards scheduled to disappear in October is the Technical Board, which has been responsible for the management and support of the Specialist group network for some years. That does not indicate any lessening of the importance of the Groups to the life of the Society – indeed quite the opposite. The move towards Knowledge Services as a main strand of acre is a clear recognition of the value of the groups as a major part of the the and an understanding of the need to improve the support

As from October, responsibility for the Groups will reside with the Member Services Board, as also will that for the Branches. The Board will have overall responsibility for the Specialist group network but we expect the day to day management issues to be handled by an Executive Committee elected by an annual meeting of all the Groups to be held before the end of September each year. The Chair and Vice-Chair of the committee, also elected by the annual meeting, will be members of the Member Services Board.

No changes to the composition of Council are proposed at present and the Groups will continue to nominate three representatives. Nomination will also take place at the September meeting each year.

Informal Affinity Groups

One other proposal currently under consideration involves the introduction of a new form of organisational unit that we have labelled an Informal Affinity Group. Essentially the idea is to encourage networking by making it possible for two or more members to form a group with the minimum of bureaucracy. The formation and operation of such groups would be subject to a simple set of rules:

◆ There would be no approval process but groups would be required to register before they could use the BCS logo.

◆ Any two or more members, in any grade, of the Society, would be entitled to form an Informal Affinity Group to pursue matters of common professional interest or to encourage networking.

◆ No formal constitution or rules would be prescribed for Groups and no approval would be required for their formation or disbandment. However, it would be a requirement that an Informal Affinity Group should not enter into competition with any existing Branch or Specialist Group.

◆ Groups would not be entitled to hold funds, whether provided by the Society or some external source.

◆ The Society would maintain and publish a register of all Informal Affinity Groups and any Groups would have to register in order to be recognised by the Society.

The Member Services Board would have power to revoke the registration of any Group where it considered the conduct of the Group likely to bring the Society into disrepute or where the Code of Conduct was not being properly observed. The Board would also have the power to require that a Group should apply to become a Branch or Specialist Group where it considered that status more appropriate.

New Services and Upcoming Events

Just to prove that we are not spending all our time navel gazing, some news about new services and events in prospect:

BCS Kitemark - a new scheme to recognise employers able to demonstrate commitment to best practice in IS staff development. This accreditation new service is to be launched in the the Autumn under the banner of ‘IS Quality at Work’.

BCS AGM and Lecture – This year’s AGM will be held at Church House Westminster at 3.30 pm on October 25th. It will be followed, at 6 o’clock, by a lecture to be given by Dr Doug Englebert, the developer of the mouse and hypertext links in the 1960’s. Dr Englebert will also be presented with the Society’s Lovelace Medal for a contribution of major significance in the advancement of IS.

BCS/IEE Recruitment Show – Another in the series of very successful IS recruitment events, organised jointly with the IEE, will be held at the NEC Birmingham on 26 and 27 October this year. The shows offer employers the opportunity to make 25 minute presentations and the attractions for those seeking new jobs include free entry, career seminars and CV clinic.

Advanced European Computer Driving Licence – An advanced version of ECDL is being launched to meet demand from those who have taken the basic qualification. ECDL is proving an enormous success with 1 million people across Europe holding or studying for the qualification. The figure for the UK is now around 200,000 and both the MOD and the NHS recently adopted ECDL as a standard qualification for their personnel.

New ISEB Certificate in Consultancy Practice – Work on the new ISEB certificate is nearing completion and the qualification is scheduled for launch in September. The certificate, based on the very successful BCS consultancy skills training course, will involve both written and oral examinations.

New Book Discount Scheme - A new arrangement with Pearson Education, under which BCS members receive a discount of 25% on all books ordered from their on-line bookshop.

BCS E-Bulletin – A new weekly e-mail news service has been launched by the Society, in association with Silicon.Com. This e-Bulletin is intended to complement the bi-monthly members' magazine, Computer Bulletin, and carries short, BCS and industry news items, with links to full stories on the Web. It also provides a diary of events plus links to moderated BCS discussion forum.

And Finally……………

BCS drops the UK from its URL. The BCS Web site, including details of all the services and events outlined above, will now be found at **www.bcs.org**

From the Antipodes

Bob Ashton – Australian Correspondent

Changes to Australian Copyright Legislation

On 5 March 2001, it became technically illegal for Australians to forward another person's or organisation's email to a third party or person without the permission of the originator. This applies even if the email contains only personal or non-original information and is one result of the changes to Australian Law brought about by the *Copyright Amendment (Digital Agenda) Act 2000.*

This Act is designed to update the *Copyright Act 1968* to take account of the fact that much information is now stored and sent electronically. The 1968 Act only recognised paper based documents, while the amended Act attempts to be technology neutral.

The Act has the following features:

New right of communication

Copyright holders now have the right to decide how their material may be used electronically or made available on line. This applies to video, email, web publishing, broadcasting, etc.

Stronger enforcement for copyright owners

The Act now allows copyright owners to use technological devices to protect their copyright e.g. locking or encryption devices.

Restrictions

When reproducing material, it is now an offence to remove Rights Management Information (RMI). That is, the information attached or embedded within digital material that identifies the material and it author/copyright owner or its conditions of use. For example, when forwarding an email, it is illegal to delete where and from whom the original email came from, the time it was sent etc.

Also introduced are criminal penalties and civil action avenues for "making, dealing or importing devices and services which circumvent technological copyright protection measures (eg decryption software). Exceptions are made for "permitted purposes" which can include activities by libraries, governments, educational institutions etc. Unauthorised access to encoded signals (eg Pay TV) is also covered by civil and criminal penalties.

In this area Australian legislation is following the American example.

Email and Copyright

While technically it is illegal to forward another person's email without their prior permission, it would first need to be proved that the email is an original literary work before a breach of copyright would occur.

Exceptions for all users

The Act extends the 'fair dealing' exceptions that apply in the analogue environment, where practical, to the digital arena:

Copyright material can be copied for certain purposes (research, study, criticism, reporting news) without the owner's permission, if the use constitutes fair dealing. What constitutes fair use or fair dealing depends on the portion being copied, commercial availability of the material and its effect on the market.

A user may copy 10% of an electronic text work without permission or having to consider commercial availability ***but only for research or study***.

Users are not liable for temporary reproductions made during the course of a transaction eg caching on the computer when surfing the Internet.

Readers requiring more detailed information should refer to:

Australian Copyright Council
http://www.copyright.org.au/

Copyright Agency Ltd
http://www.copyright.com.au/

Copyright Legislation
http://www.austlii.edu.au/au/legis/cth/num_act/toc-C.html

Computer Audit Specialist Group

casg

THE BRITISH COMPUTER SOCIETY

BCS

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) BCS membership number: ________________________	£15
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

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

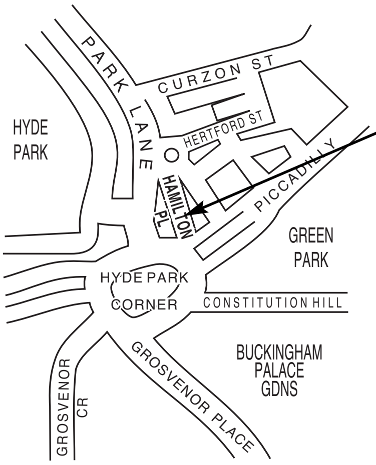
CHAIRMAN	John Bevan	Audit & Computer Security Services	01992 582439 john.bevan@virgin.net
SECRETARY	Raghu Iyer	KPMG	020 7311 6023 raghu.iyer@kpmg.co.uk
TREASURER	Mike Demetriou	CrestCo Ltd	020 7849 0000 mike.demetriou@crestco.co.uk
MEMBERSHIP SECRETARY	Vacant		
JOURNAL EDITOR	John Mitchell	LHS Business 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

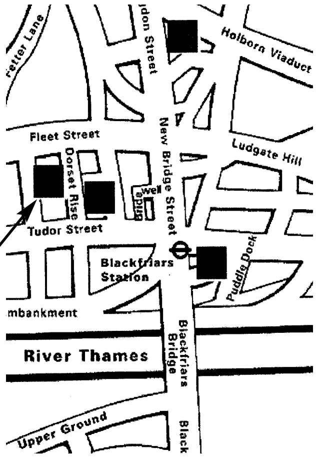
Venue for Full Day Technical Briefings



Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ

Venue for Late Afternoon Meetings

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 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