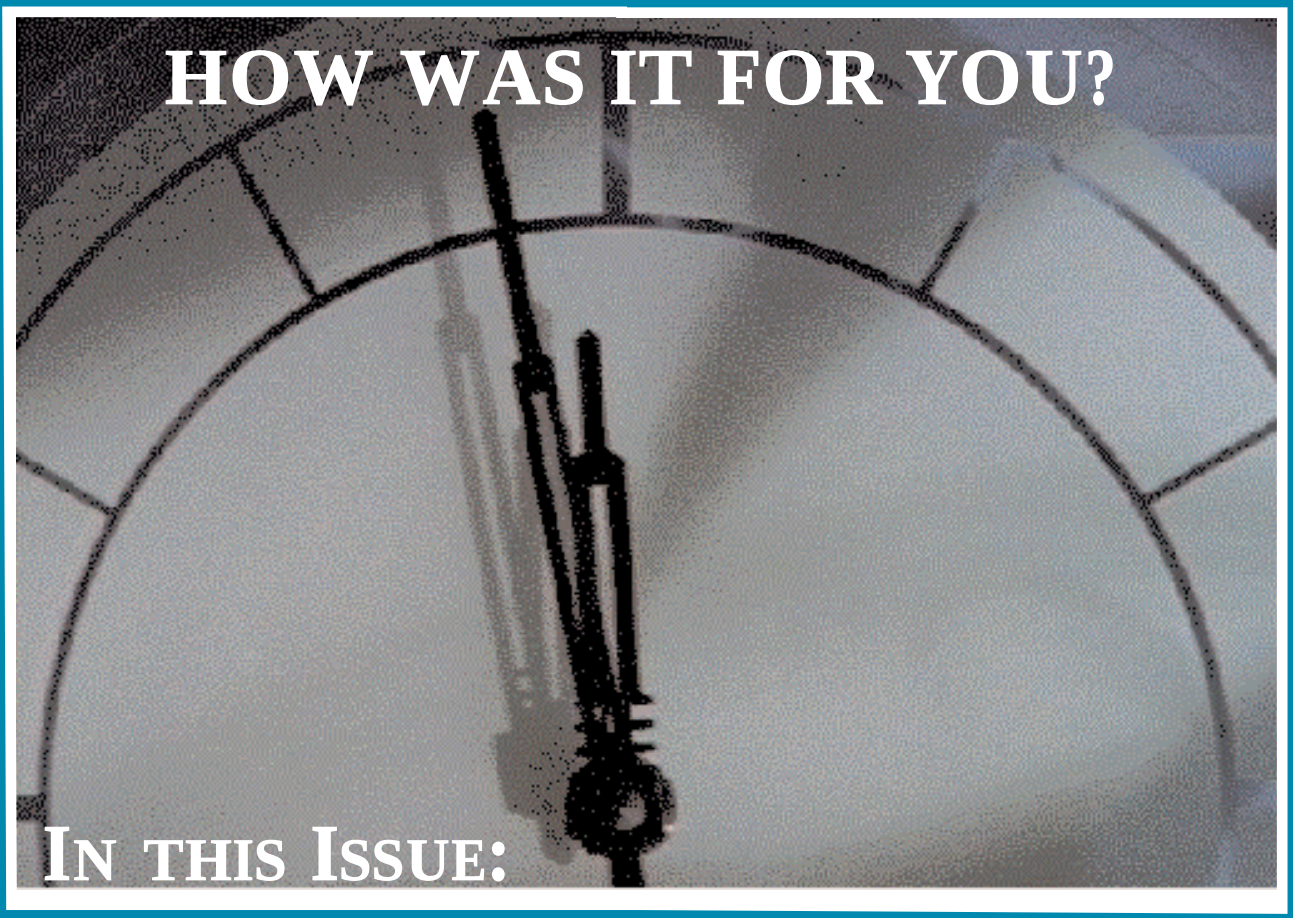
ISSN 1356-0735

DATAWATCH

VOL. 43, JAN/FEB 2000



IN THIS ISSUE:

THE QUARTERLY MAGAZINE OF ISACA LONDON CHAPTER

VOLUME 43, JAN/FEB 2000

DATAWATCH

is a quarterly magazine
published by the

Information Systems Audit and Control Association

London Chapter

To advertise:
Call Nancy Watt on:
01487 815705
or Email:
Isacalondn@aol.com
Website: ISACA.org.uk/London

Chapter Office:
10 Drayhorse Road
Ramsey, Huntingdon
Cambs PE17 1SD

DATAWATCH is published by the Information Systems Audit and Control Association London Chapter, membership of the chapter entitles one to receive an annual subscription to DATAWATCH.

In this issue:

FEATURES

REGULARS

PLUS

ISACA London Chapter Committee 1999/2000

PRESIDENT
John Mitchell
LHS Business Consultancy
01707 851454
Lhs@lhscontrol.co.uk

VICE PRESIDENT
Steve Bailey
Steve Bailey Associates
01480 432602
Spart@compuserve.com

TREASURER
Archie Watt
BDO Stoy Hayward
0171 893 2671
Archie.Watt@bdo.co.uk

SECRETARY
Charles Mansour
The Woolwich
0181 298 5646
Charles.Mansour@woolwich.co.uk

MEMBERSHIP
Kamal Khan
Sanwa Bank Ltd
0171 330 5522
kamal.khan@sanwabank.co.uk

PUBLICATIONS
Annabel Lane
Nestle UK Ltd
0181 667 6530
annabel.lane@nestlegb.nestle.com

SIGS
John Hunter
HLB International
01635 248944
mailbox@jhunter.u-net.com

SIGS/LIBRARY
Bill Hawkins
Corporation of London
0207 332 1296
Bill.Hawkins@corpoflondon.gov.uk

MARKETING
Derek Oliver
Ravenswood Consultants
01268 794556
consultants@ravenswood.co.uk

EVENTS
Karen Sharpe
Deloitte & Touche

karen.sharpe@deloitte.co.uk

CISA CO-ORDINATOR
David Spaven
KPMG
0171 311 5620
David.Spaven@kpmg.co.uk

PAST PRESIDENT
Gerry Penfold
KPMG
0171 311 8489
Gerry.Penfold@kpmg.co.uk

WEBMASTER
Allan Boardman

01732 462 133
allan@internetworking4u.co.uk

CHAPTER OFFICE
Nancy Watt
10 Drayhorse Road, Ramsey, Huntingdon, Cambs, PE17 1SD
Tel/Fax: 01487 815705

WEBSITE:
WWW.ISACA.ORG.UK/LONDON
Email:
Isacalondn@aol.com

ISACA Northern UK Committee (officers only)

PRESIDENT
Ray Butler
HM Customs & Excise
0161 827 0875
rbutler.c&e.cau@gtnet.gov.uk

VICE PRESIDENT
Robert Newbould
British Steel
01709 825479
bob_newbould@technology.britishsteel.co.uk

TREASURER
Gillian Peschke
Pricewaterhouse Coopers
0113 289 4273
gillian.peschke@uk.pwcglobal.com

MEMBERSHIP
Lynn Lawton
KPMG
0161 838 4000
Lynn.Lawton@kpmg.co.uk

CISA CO-ORDINATOR
Alan Rainford
Axa Insurance
01253 662782
alan_rainford@gre-group.e-mail.com

WEB MASTER
Peter McCready
MBNA International Bank
01244 672000
macriada@btinternet.com

ACADEMIC RELATIONS
Mike O'Hara
University of Salford
0161 295 5665
m.j.ohara@iti.salford.ac.uk

WEBSITE:

WWW.ISACA.ORG.UK/NORTHERN

ISACA Central UK Committee (officers only)

PRESIDENT
Mike Hughes
KPMG
0121 232 3207

VICE PRESIDENT/CISA
Simon Parker
Canada Life
01707 422064

SECRETARY
Steven Babb
KPMG
0121 232 3213

TREASURER
Geoff Adey
KPMG
0121 232 3202

PAST PRESIDENT
James Whittaker
BT
0121 230 2214

WEBSITE:

WWW.ISACA.ORG.UK/CENTRAL

The Editor's Chair

The "Millennium Bug" - Apocalypse or Apocrypha?

By Annabel Lane

By the time you read this you will probably be bored with being wished a Happy New Millennium, but as this is our first edition of the new millennium (depending on when you count it from) it's my duty to wish you all the best in the new year.

We have made it anyway, and confounded the survivalists, cultists and other prophets of doom as the world and the economy are still functioning. Well, they were at the time of going to print anyway. There are of course plenty of people around who say that the lack of serious Y2k problems means that we wasted our time and money and put far too much effort into beating a millennium bug that was never really as threatening as the hype made out, and that a lot of consultants have made monkeys out of us all, pocketed their inflated earnings and retired to the Bahamas to dream up the next panic.

I can't subscribe to that point of view. I have learned a great deal over the last couple of years through my involvement in my own company's Year 2000 project, and not just how to spell millennium! There are a great number of people who claim that the knowledge gained undertaking and auditing these projects won't ever be used again - well I don't agree with that. It's given quite a few auditors a chance to review, and in some cases participate in, what has been one of their company's biggest and most important projects ever. It's been a chance to be seen as working with IS and other departments rather than coming along after the event and criticising what has been done. A great many of us have gained detailed knowledge of systems and areas within our companies that we wouldn't have otherwise seen. And for the company itself, the amount of work that has gone into such projects in many cases can be used as a basis for continued improvement. A great many firms have reviewed the use for and in some cases got rid of systems and hardware that had been plodding along under utilised for some time, thus saving themselves money and resources - for example from maintaining mainframe systems that have now been switched off. It has given many companies the impetus they needed to justify replacing old equipment and to catalogue hardware, software, machinery, etc that they have retained thus making management of these resources more efficient in future, and giving us all greater confidence in their reliability.

Having said that, it is a great prospect now to be able to return to a more normal audit timetable and to have more flavours of IS projects to pick from in the audit selection box. We're not out of the woods yet by any means and I'll be glad when February 29th has come and gone for starters, but I think we should take pride in the work that has been done and in our part in it when we think what could have happened.

What do you think? If you disagree, or even agree, drop the Editor a line either to my personal address or to the Chapter Office. We'll publish the best we receive and award a prize for the star letter. And all the best to you for the new year. It's going to be an exciting one, I'm sure!

From the President

By John Mitchell

If you are reading this in January 2000, then the lights did not go totally out and any flickers are being dealt with by the lawyers. You must realise that I am penning this in December 1999 as a result of a dictate by the big boss of the editorial panel (Annabel Lane) to get the copy ready just in case the lights do go out.

So what has happened since my last column? Well, another trip on behalf of the Chapter. This time to less than sunny Manchester for a weekend meeting of European Presidents to hammer out more local things than were discussed at the Global Leadership conference in Denver back in July. Change of scene, change of weather and much more easily managed as only a score of Presidents came over. Our Northern Chapter cousins, who had persuaded KPMG to provide the facilities, very ably hosted the whole thing. Very interesting to re-aquaint myself with some of the people I had met in Denver and to meet several more who hadn't been able to make that particular venue. Amazing people. The working language was English in deference (or was it pity) to us poor tongue tied Brits, but at the drop of the hat the rest could switch into any number of other languages. I estimate that each President could handle about three languages apiece at quite a technical level. Me? Well a smattering of poor German, but I do speak excellent COBOL, which surprised some of the younger Presidents who view COBOL as the equivalent of medieval Dutch. They are all into Visual Basic and C++. I also wondered what the extra plus was for. It seems it means it's turbo charged. A bit like go faster stripes on the kiddies' hot hatches.

Ah, back to the point. One of the things we discussed was the role of the CISA co-ordinator. One of the more demanding jobs on any Chapter Board, but often the one where some poor unsuspecting sap (sorry David Spaven), gets lured onto the Board with promises of dazzling stardom, only to find that the job is the equivalent of mucking out the stables while the occupants are snapping at your ankles. So it was agreed that London would develop and host a CISA co-ordinator's training weekend sometime this year. Should be fun, shouldn't it David?

Whilst up in Manchester I got together with Ray Butler and Mike Hughes (Northern and Central Chapters respectively) to hammer out a memorandum of understanding between our three Chapters. What this means in practice is that any member of any Chapter can get entry to any Chapter event at the local member's rate. So if it is free for them, it's free for us and vice versa. We don't expect hoards of visiting members, but any that do turn up will receive a warm welcome from the local Chapter. Likewise if you are in the Manchester or Birmingham areas, check out with the locals if a meeting is scheduled (contact details on page 2) and make yourself known. Superb hospitality north of the Watford Gap if my experience is anything to go by.

One other thing that was raised in Manchester was the need for assessors for proposed content for ISACA's great Global Information Repository (GIR). If any of you have used the various web search engines, you will be well aware of the problem of indiscriminate information. Enter the key word security and 360 million references are presented. The whole idea of the GIR is to provide a list of refereed papers on all aspects of information security and control. The problem at the moment is a critical lack of referees. So this is the cunning plan. Every one of you should email Peter Hill (pthill@iafrica.com), the South African President, who is co-ordinating things asking for a GIR Volunteer Request Form. Once registered you can start earning those precious CPE hours that are so valuable to the 50% of you who are CISA qualified. Every little helps and last year we had one member who was in dire straights as a result of not having enough hours to keep the designation.

One final point. We have just co-opted Allan Boardman to the Committee as Web Master. We have been aware for some time that our tentative entry into web publishing should now be expanded and Allan is the person for the job. Welcome aboard Allan.

Finally, it may be late, but a very happy and prosperous New Year to you all. Please come to the meetings if you are in town. I also look forward to seeing you.

Membership Matters

By Kamal Khan

The ISACA London Chapter currently has 657 members, some of whom made members after successfully passing the CISA exam earlier this year. Hopefully all of you temporary members will by now have realised how value-packed membership of the Association is: high quality journals, conferences, seminars, workshops, free monthly meetings giving you the opportunity to pick up CPE points at no cost (once you gain CISA certification you need at least 20 contact hours per year to retain it), and the opportunity to network with others in your profession. So please, seriously consider renewing your membership, it will be well worth your while.

Finally, it is very important to make sure we don't lose touch with you as you move or change jobs. You can do this very easily directly from the Members Only area of the International website at http://www.isaca.org (you will be sent details about how to access this area with your 2000/2001 membership card).

London Chapter Events 1999-2000

The Extended Enterprise

"No man is an island" and neither is a modern enterprise. All kinds of businesses and public sector organisations have embraced networks and distributed computing within the boundaries of their organisations. With the explosion of the internet, business to business e-commerce is becoming easier and cheaper. Links to customers, suppliers and other third parties such as banks or information providers are increasing. Business processes are reaching out into other organisations, not only for transaction processing (e.g. ordering, invoicing, distribution, payments) but also for business planning (e.g. suppliers accessing customers' systems for demand planning or customers accessing suppliers systems for product information).

Technology is also enabling other efficiencies in areas such as procurement, through the use of smart cards for example, for high volume, low value purchases.

The era of e-commerce and the latest technological developments makes the concept of the Enterprise a reality today. This is a growing challenge for IS Audit and Security professionals, especially as the high performance companies of tomorrow will be exploiting the concept rapidly, challenging our current thinking on IT governance, risk management and control. What sort of enterprise will we be auditing in the next few years? The London Chapter's 1999/2000 programme of events aims to explore this theme and propose some of the answers - so come along and help shape the future!

16 September 1999
The High Performance Co
Gerry Penfold

21 October 1999
BS7799/C:Cure
Derek Oliver

18 November 1999
Development Issues in the Extended Enterprise
Barbara James

16 December 1999
Christmas Meeting
Annabel Lane & Andy Farrington

20 January 2000
Internet Security
Anand Singh

17 February 2000
PKI
Zergo Baltimore

16 March 2000
Digital Signatures
Fred Piper & John Mitchell

20 April 2000
Intrusion Detection
ISS

18 May 2000
AGM &
Penetration Testing
Steve Bailey

15 June 2000
Contingency Planning for the Extended Enterprise
TBA

All meetings will take place at the offices of KPMG, 8 Salisbury Square, London EC4 commencing at 4.30pm. Meetings are free to members, a charge of £20 will be made to non-members.

Is your business c:cure?

By Derek Oliver, CISA, CFE

C:cure is the name of a scheme launched in the United Kingdom in April, 1998 to provide certification of compliance with BS7799. Now, that's probably a somewhat meaningless statement to most readers of the "Journal" so, before you turn the page, I'd better give a brief overview.

In short, certification against BS7799 is intended to provide confidence in your company, whether it's to your suppliers and customers in inter-company trading, to your shareholders or to the general public. Flying the **c:cure** flag will say to any interested party . . . . . .

"This enterprise:

- ✦ recognises the need for information security
- ✦ has completed a risk assessment programme
- ✦ has implemented controls to address the risks"

What is BS7799?

BS7799, more fully the British Standards Institute (BSI) standard number 7799, is entitled the **Code of Practice for Information Security Management**. The document was first published in February 1995, with the International Standard Book Number (ISBN) 0-580-23642-0, by a BSI working party, which was sponsored by the British Government's Department of Trade and Industry (DTI) and included representatives from many large, commercial organisations such as British Oxygen, Prudential Assurance, British Telecommunications, Midland Bank, Nationwide Building Society, Shell International Petroleum and Shell U.K. as well as the British Computer Society (BCS) and the government's Central Computer and Telecommunications Agency (CCTA).

The BSI is the independent national body responsible for preparing British standards. It presents the United Kingdom's view on standards in Europe and at the international level and is incorporated by Royal Charter.

The working party took as their model the basic components of information security which are essential to maintain the competitive edge, cash flow and profitability of a business: Confidentiality; Integrity and Availability. Their stated objectives were:

- ✦ to provide a common basis for companies to develop, implement and measure effective security management practice and
- ✦ to provide confidence in inter-company trading.

As a code of practice, the standard took the form of guidance and recommendations rather than a clearly defined specification and, initially, was not a document that was intended to form a set of minimum requirements against which compliance could be assessed and accredited. The standard makes clear that "there is no single best structure for security guidance" as each of the defined categories of user will have different security requirements for their individual status; different problems, risks, threats and priorities depending upon the particular function, organisation, business or computing environment.

Soon after publication it became clear that accredited certification would require something more than the guidelines of a "Code of Practice" and a project was initiated to consult with:

- ✦ **End User Businesses** - organizations who would be likely to seek accreditation
- ✦ **Business and Trade Associations** - representatives of large and small enterprises
- ✦ **Certification Organisations** - such as the International Register of Certified Auditors (IRCA) and the U.K. Accreditation Service (UKAS)
- ✦ **Professional Associations** - including ISACA, the British Computer Society and IIA

The culmination of this period of consultation, in which the ISACA London Chapter were active, was the publication of **BS7799 Part 2: Specification for Information Management Systems**. It is against the precise requirements of Part 2 that an organisation will be measured for compliance.

Why was a Standard considered necessary ?

According to a DTI statement in

1993, "the threats are expected to become more widespread, more ambitious and more sophisticated". This is not the place to discuss computer crime and abuse in depth, but it is worth recalling briefly the number of reported attacks on, or abuse of computer systems in recent years and the number of "disasters", both man-made and natural, that have put computer-dependent businesses under threat.

Information Technology systems and communications networks may be the target of a range of serious threats including computer-based fraud, espionage, sabotage, vandalism and other sources of failure or disaster, not to forget good, old fashioned theft. Recent years have seen the emergence of increasingly sophisticated threats in the form of "hackers" and computer "viruses".

At the same time, the increasing dependence upon computer systems and services mean that almost every organisation, from multi-national corporations to clubs and associations, are becoming more and more vulnerable to security threats. The growth of networking and the attractions of the Internet present new opportunities for unauthorised access to computer systems and the trend for "downsizing", the decentralisation of computer processing in favour of distributed systems, reduces the ability for central control of security measures, both physical and logical.

How is the Standard Structured?

Both the Code of Practice (Part 1) and the Specification (Part 2) are divided into ten distinct sections :

- The Information Security Policy
- Security Organisation
- Asset Clarification and Control
- Personnel Security
- Physical and Environmental Security
- Computer and Network Management
- Systems Access Control
- Systems Development and Maintenance
- Business Continuity Planning
- Compliance

Each section comprises a comprehensive set of controls which are based upon those practised and enforced by the business organisations represented on the working party and, thereby, regarded as reasonably common practices within the U.K. The sections contain a series of control objectives and associated control measures intending to counter, or at least minimise, perceived threats. Each section in the Code of Practice is also associated with one of ten **key controls**. These are :

1. *A written policy document must be available to all employees responsible for information security.*

The standard requires that every business should have a formal statement of its policy regarding the security of its information. This is, rightly, regarded as the foundation stone of all control procedures as well as the supporting authority for those persons empowered to enforce them.

2. *Responsibility for the protection of individual assets and for carrying out specific security processes must be explicitly defined.*

However a business defines its management structure, there must be a person or team who have clearly defined responsibility for various aspects of security. This may be divided, for example, between three specific control principles, Physical Security; Logical Security (computer system access control) and Change Management (the control of changes to production processes).

3. Users should be given adequate security education and technical training.

All employees should understand their role in the overall security of the business. This is best achieved by providing initial training in the requirements, for example, of the Security Policy with regular education sessions where various elements of security are discussed.

4. Security incidents must be reported through the correct channels as quickly as possible.

Another essential, personnel issue. If incidents are quickly reported, action can be taken by the appropriate authorities to minimise the risk to the business by, for example, the prevention of further unauthorised access and the detection and identification of any intruder. Again, this implies not only that "correct channels" must be in place but also that all employees are aware of those channels through education and regular communications.

5. Virus detection and protection measures and appropriate user awareness procedures must be implemented.

It is unbelievable the damage that this evil invention can do, or how quickly a virus can spread throughout a network. Yet again, this key requirement requires not only the need for virus detection software to be in place but also that users are educated in the dangers and have procedures to ensure that they do not use any medium which can introduce infection, such as untested floppy disks.

6. There must be a managed process in place for developing

and maintaining business continuity plans across the company.

The Business Continuity Plan, or Contingency Plan, is, quite simply, a commercial necessity wherever a business has any degree of dependence upon information systems. It must also, however, reflect those manual procedures which may need to be restored following a "disaster" and, above all, it cannot be considered proven until it has been tested and cannot be considered effective unless those tests are repeated at regular intervals.

7. Copyright material must not be copied without the owner's consent.

In the U.K., the Copyright, Designs and Patents Act, 1988, makes the copying of software without the explicit consent of the owner an illegal act. Both the Federation Against Software Theft (FAST) and the Business Software Alliance (BSA) investigate such incidents and will prosecute offenders, even large businesses, with the intention of gaining the maximum publicity to protect their members. This is an essential element of the Security Policy as such publicity can cause serious damage to the "corporate image", apart from the financial penalties that may be imposed.

8. Important company records must be safeguarded from loss, destruction and falsification.

This is, surely, a simple, basic fact of life for corporate information. In terms of procedures, this means controls to ensure that important records are backed-up, i.e. current security copies are taken and securely stored; that access locks are set to prevent accidental or deliberate deletion and that access restrictions prevent unauthorised amendment.

9. Applications handling personal data (on individuals) must comply with data protection legislation and principles.

In the U.K., this relates specifically to the Data Protection Act, 1984 (and 1998). This legislation, complying with European Union directives, requires many of the principles discussed in this paper to be applied to all data of a "personal" nature and requires all businesses handling such data to register with the appropriate authority and to comply with the legal requirements.

10. Systems must be regularly reviewed in order to ensure compliance with Company security policies and standards.

Needless to say, the reason why this is regarded as a key control is to ensure that nobody initiates control procedures then relies upon them to be observed without verification or believes that the many changes that can affect both a business and a processing system will not affect the controls!

Critical Success Factors

The successful implementation of information security within any organisation is to a large extent dependent upon a number of factors. Security objectives and activities must be based upon definitive business objectives. If employees at all levels do not understand the need for a control procedure or for security awareness, then the procedures may be circumvented or, at least, not effective and security may be compromised.

The successful enforcement of meaningful controls is dependent upon full and visible endorsement by Senior Management at the highest level. If line managers and staff believe that the corporate standards are really guidelines laid out by a fellow manager rather than a directive from the top, they may be laid open to local interpretation which, again, may reduce their effective or efficient implementation.

The security risks to which the business may be exposed must be fully evaluated and understood. There are many methods of performing risk analysis, both formal and informal; whatever method is used, it should evaluate every defined "asset" of the business and identify its threats and vulnerabilities. The analysis should involve many employees across the management structure to ensure that, so far as is possible, all potential threats are identified and classified and that the final analysis is accepted and understood by all staff.

Security must be "marketed". Whether it be by a programme of education or training or by regular communications, discussion forums etc., it is essential that every employee is aware of their role within the corporate security structure and of the procedures that they may have to initiate.

Comprehensive guidance must be given to both staff and contractors. The Security Policy should not be a one-off, all-encompassing management document; these tend to be "filed" and forgotten. The policy should be a "living" document which is regularly reviewed and is published in a simple, easily readable form that can be provided to all staff, permanent and temporary, so that they know exactly what the company requires of them and, preferably, why.

So much for BS7799 as a set of guidelines for the management of security, its origins, development, content and structure. The Code of Practice, published on February 15th, 1995, has proved of immense value to auditors and security personnel for

many major companies in the U.K. who have succeeded in establishing a programme of security "Health Checks" within their businesses to evaluate their degree of compliance with the guidelines. Formal accreditation by certified BS7799 auditors providing a certificate of compliance to those businesses that qualify was the next logical step.

Where are we now?

Formal accreditation against BS7799 was announced by the British Government's Minister for Information Technology early in April, 1998. Since then, the mechanisms for applying for accreditation, auditing compliance and issuing certificates have been developed.

The BSI, through their IT and Telecomms Division "BSI-DISC" have published a comprehensive series of books on various aspects of accreditation, from a Management Summary through Risk Analysis to a detailed Auditor Guide. (A full, current list is available on the BSI web site - see the end of this article for details).

At the moment, the IRCA is in the process of certifying c:cure auditors at three levels, depending upon the relevant qualifications and experience of the individual. Auditor certification will also require, for all but the most experienced individuals, passing an examination in the standards plus an interview panel, made up of "high profile", experienced audit and security professionals.

Concurrently, UKAS is in discussions with organisations who intend to employ these certified auditors to evaluate compliance and issue certificates. Unsurprisingly, these will be known as Certifying Bodies.

The DTI has set up a BS7799 User Group, comprising all interested parties, including businesses considering accreditation and representative associations, including ISACA. The intention is that this group will shortly cut its' association with the Government and be run by a Steering Committee. The ISACA London Chapter has already been invited to provide a representative for this committee as well as the scheme steering group.

Who's Interested?

It must be said that there is not yet a rush of organisations wishing to sign up for the **c:cure** scheme. On the other hand, the meetings of the User Group to date have seen representation from more than 180 interested organisations and this number is confidently expected to grow.

The international business continuity organisation "Survive!" have also created a BS7799 Special Interest Group, which is similarly well attended and growing.

Once the first certificates have been issued, there is certain to be a great deal of public and commercial pressure for all large organisations to have the epithet "BS7799 Certified" to demonstrate their commitment and adherence to information security management standards.

Banks and financial institutions may well be the first to find they need certification to gain and retain customer confidence: the implication will then be that their suppliers will be required to comply to keep that confidence throughout the business chain.

Government departments, especially those dealing with confidential, personal information or taxation, will surely be expected to comply.

The continuing growth of Electronic Data Interchange (EDI) must encourage compliance with BS7799 as the natural indicator of "trusted party" status. After all, it's important to know that the recipient of your data will treat it with the same level of security as you do yourselves. International Implications.

Although BS7799 is a British standard, it has already been adopted as the basis for national standards in many other parts of both Western and Eastern Europe as well as more distant countries.

The Steering Group hope that in due time the standard will be developed with a more international flavour and be adopted by the International Standards Organisation (ISO) so that certification of compliance becomes internationally recognised. To this end, the "Guidelines" (BS7799 Part 1) have already been re-drafted to replace all UK-specific references, such as requirement to comply with British legislation, with a more conceptual form of words.

Currently, responses to the draft re-write, including those from the ISACA London Chapter, are being consolidated and assessed in preparation for a formal reissue.

Interested?

Further information on BS7799 and the c:cure certification scheme as well as details of available publications and guidebooks, can be obtained from their website at www.c_cure.org or by good, old snail-mail from:

c:cure Scheme Manager,
BSI - DISC,
389, Chiswick High Road,
London, W4 4AL,
United Kingdom.

Tel: +44 (0)181 996 7408
Fax: +44 (0)181 996 7448

Derek J. Oliver is IS Audit & Security Director of Ravenswood Consultants Limited. He is a Certified Information Systems Auditor and a Certified Fraud Examiner; a Member of the British Computer Society and Fellow of the Institution of Analysts and Programmers, he is also a Freeman of the City of London. He is past President of the ISACA London Chapter and is a current member of the CISA Certification Board.

NETWATCH

By Annabel Lane, Nestle Plc

Well, the celebrations have been and gone and life seems to be carrying on as normal for me. Mind you this bunker in the Scottish Highlands is so well equipped that I can even surf the net and submit my Netwatch column from it……!

Talking of upheaval, I wanted to flag up to you the fact that there is now a new way in to the London Chapter web site.

www.isaca.org.uk

Accessing this URL will give you the ability to link through to the web sites of any of the three current UK ISACA chapters. Clicking on the London link takes you through the ISACA London Chapter web site which I have mentioned (or do I mean plugged?) before. But you are also offered a link to the central and northern chapters' sites. So I thought I'd take a look.

The Northern Chapter web site opens up with some information on an event taking place in July, hosted at the University of Greenwich by the European Spreadsheet risks International Group. There is a list of officers you can contact and the President has a message posted which tells you of the advantages of ISACA membership. But of course, you all know that already….If you were interested in attending the next meeting in their events schedule the details are here, as is some information on CISA, as well as links to other useful sites and list servers you can apply to to join in discussions and share knowledge.

The Central chapter has a few additional features of interest. It is possible to view the details of the next and last event and if you have the relevant id and password you can access the slides from the latter. They have announced that they will be launching a "members only" page shortly, which sounds interesting. There is a search engine enabling you to search the site or the web itself and plenty of link sites to hook up to. On the CISA page there is a paper of 25 sample questions. I dare you to give them a try and come up with your score. It made me feel very inadequate I can tell you!

For the rest of my journey into Cyberspace today I decided to take the lead from the London Chapter's events programme and consider some sites with ecommerce/security connections.

http://www.antionline.com/

Despite the name, Antionline are a foundation dedicated to education in security matters - not Luddites who want us all off the Web! This site contains links to items of security news, weekly quick tips and a mailbag of questions asked. They seem to enjoy baiting the hacking community as one of their links is to a list of attempted hacks into their network against which they list the address of the perpetrator wherever possible. They also offer you the opportunity to obtain a full security report of your system by entering your email address and hitting "go". "One of our systems will scan your computer remotely, then e-mail you with a full security report of your system. We'll tell you of any security problems you have, and how to fix them". I didn't try this one personally, though I was tempted to have a chat with their very avuncular looking security expert "Bub" who will answer all your questions on the subject of security.

An interesting link is the Antionline "Eye" which appears to scan other sites for activity of interest and report on it. It tells you when some of the best known hacking sites, like Cult of the Dead Cow were last updated, and there are other links to sites dealing with encryption, privacy, etc, and even links to all sorts of "underground" hacking sites, some of which have intriguing names!d

http://www.cnn.com/TECH/special

s/hackers

This rather whetted my appetite along the "know your enemy" type of lines, and I thought this site was intriguing. It's run by CNN and as you might expect specialises in news stories. You can participate in a discussion on the definition of hacking and read articles on the likelihood of serious cyber attacks "on the scale of Pearl Harbour" and what Friday night is like in the hacker underground. There's quite an interesting article on what hackers do and who they are really likely to be, as well as links to other sites of interest on subjects such as cyber terrorism and computer security.

http://www.sse.ie/securitynews.html

Also on the lines of security news is this site which comes from SSE, Secure Solutions Experts. This one gathers together all the latest articles electronically so if you are looking for news on the latest worm or information on a security breach you have heard about and want to investigate further, this could be a good starting point. Clicking onto a subject, like Security, or Cryptography sends you onto a list of articles on those subject which you can link to to find the latest published articles.

http://www.clark.net/pub/mjr/pubs/fwfaq/index.htm

Firewalls. Something that gets a lot of use in the extended enterprise area as a means of restricting traffic into a network - also a very important security control generally. That, coupled with the fact that I like to include sites that are useful to those of us with limited knowledge of certain technical areas (and as you know I include myself in that) meant that I wanted to include this site this time.

Its title is "An Internet Firewalls FAQ site" and it starts right at the basis of what a firewall actually is, why you would want to consider having one and what they can protect you against. Then it gets onto relatively detailed information on design decisions a company needs to take on its firewall and even configs for a CISCO filtering router. It will tell you the basics of what a DMZ is, a proxy server, and even what some of the attacks are against which you might want to defend your network. And if all this information isn't enough for you, there are books to purchase and other linked sites to visit.

I've bookmarked this one myself as I think it's a really good basic resource. If they ask you to do a firewall review and you feel a bit non plussed, I would recommend this as a place to start.

http://www.cerias.purdue.edu/coast/hotlist/

This is another site which pulls together such a wide range of links to other sites that I can't possibly do them justice in my small column! The hotlist directory on the left hand side is the place to start - pick your subject from security organisations, physical security, world wide web security, computer viruses, computer ethics, you name it. Selecting one of these brings up a list of sites on that subject on the right. For example, under the subject of computer viruses are sites ranging for Dr Solomons toolkit, through sites exposing virus hoaxes, and virus alert calendars. There is a site on macro viruses - surely most of us have had one of these by now - and it actually tells you hoe to get rid of the little blighter.

Talking of viruses and hoaxes, my coffee break site for this issue is on the same theme:

http://ciac.llnl.gov/ciac/CIACHoaxes.html#goodspoof

It always makes me smile when a very well meaning friend sends me details of a horrible new virus that will do God knows what to your hard drive, career and personal life. The give away for me is usually at the end if it says and tell everyone you know about this terrible threat to mankind. Well, I'm not the only cynic who gets fed up with it all! Try this URL and read Patrick J Rothfuss's spoof on the infamous "Good times" virus that never really existed, but knew it as well as if it had!

Bill Clinton, Tony Blair and Bill Gates all die in a plane crash. They are standing before God, seated on his throne. God asks Tony: "What do you believe?" Tony says: "I believe in the earth. I believe if we don't protect it, the whole earth will die." God says: "I like that, come sit at my left. Bill Clinton, what do you believe?" Bill Clinton says: "I believe in people. I believe the people should be empowered. I believe no one has the right to tell someone else what to do." God says: "I like that, come sit on my right. OK Bill Gates, what do you believe?" Bill Gates says: "I believe you're in my seat."

INTERNET RESOURCE LIST

AUDIT:

www.isaca.org.uk
www.isaca.org
www.auditnet.org
www.acua.org
www.gallaudet.edu/~auditweb/index.html
www.gallaudet.edu/~auditweb/kits.html
www.anao.gov.au/reports.html
www.theiia.org
www.iia.org.uk
http://www.methodware.com/links/
www.itaudit.org

SECURITY:

www.cert.org
ciac.llnl.gov/ciac/
spam.abuse.net
www.cl.cam.ac.uk/spam/
www.iki.fi/liw/mailfilter.html
csrc.nist.gov/secpubs/unix_security_checklist.txt
www/ntsecurity.net/
www.first.org
www.cauce.org/
http://www.securityportal.com/
http://www.antionline.com/
http://www.cerias.purdue.edu/coast/hotlist/
http://www.sse.ie/securitynews.html

COMPUTER COMPANIES AND SYSTEMS:

www.microsoft.com
www.alw.nih.gov
ntresearch.com/
www.acl.com/audit/audit2.htm
www.cica.ca/idea/index.htm

OTHER ORGANISATIONS:

www.bcs.org.uk
http://www.auditserve.com/frmain.htm
www.coactiveconnection.com/
www.mc2consulting.com/

HACKERS AND VIRUSES:

www.2600.com/mindex.html
www.sophos.com/virusinfo
www.drsolomon.com/vircen
http://www.cnn.com/TECH/specials/hackers
http://www.l0pht.com/

AREAS OF AUDIT INTEREST:

www.disastercenter.com/audit.htm
http://www.teleport.com/~jhw/csa/
http://www.clark.net/pub/mjr/pubs/fwfaq/index.htm

NEW!

E-Commerce Security: A Global Status Report

ISACA's mission in this project is to provide the link between the control concerns of management and the implementation of controls in information systems. This is the first part of a four-phase project.

Deloitte & Touche, commissioned by ISACF™, interviewed 150 companies and surveyed ISACA members in 46 countries. Tables illustrate such issues as:

- the significance of types of E-Commerce by industry and region,
- informational versus transactional E-Commerce activities by region and industry
- the perception of E-Commerce risks of availability, confidentiality and integrity.

Graphs depict who is responsible for E-Commerce as well as who sets out and enforces policy. Data on policy and control satisfaction and the use of types of encryption are analysed.

The next phase, a Global Best Practices perspective on E-Commerce security, will be available in the first quarter of 2000. At that time, production will begin on the third phase, a series of eight technical reference guides on various technologies and practices that represent the architecture of E-Commerce.

The final phase, a series of case studies on E-Commerce security, will appear in mid-2000.

E-Commerce Security: A Global Status Report is available to members for US$35 (US$50 to non-members). For more information or to order e-mail bookstore@isaca.org

NEWSROUND

By "The Newshound"

How Was it for you?

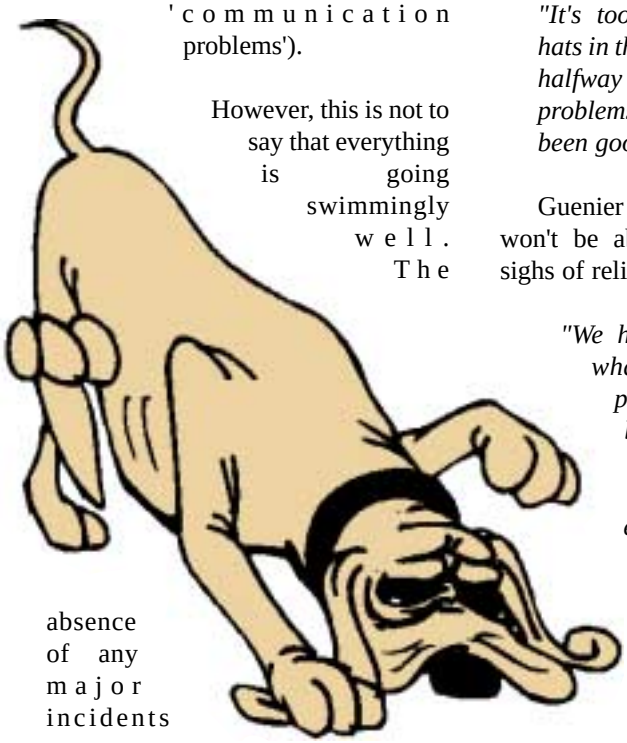
So the big day is now over and the Y2K bug seems most conspicuous by it's absence. We had a few red faces at HSBC when RACAL branded credit card terminals failed, some power plant problems in Japan and few hospital equipment failures in Scandinavia. As an exercise in irony the Government's own Year 2000 Information Centre web site showing a date of 1900 for a few hours in the New Year can hardly be bettered. Fortunately an eagle eyed, and obviously sober, site administrator corrected the problem before it hit the national press.

A bank in Germany proved that good will to all men does not apply to the financial services sector as miscalculated interest based upon the date change resulted in a credit of £4m to a customers account. It managed to contain the problem before any of it was spent.

A few mothers made a bid for stardom by phoning the Sunday Sport claiming to have given birth to 100 year old children and someone in New York was charged $91,000 for returning a video a century late.

The saddest story concerns a Bangkok street vendor who, convinced her bank would fail, withdrew her life savings of 100,000 baht, (about £1,600), and kept the money safely tucked under her mattress at home. Unfortunately an unruly millennial firework landed on the roof of her house setting it ablaze and reducing all her possessions to ash - including the money.

To date no planes bound for Washington have landed in Cairo and no satellites have fallen out of the sky, (although the Pentagon did admit to a few 'communication problems').



However, this is not to say that everything is going swimmingly well. The absence of any major incidents appears to have provoked outbreaks of apoplexy in some company boardrooms with witch-hunts already underway to punish the perpetrators of such vast unnecessary expenditure.

One could of course take the view that Y2K appears, to date at least, to be one computer project that actually delivered on time and met its objectives. Perhaps corporate culture needed some hype to shake it out of it's complacency and spur it into action. Perhaps we should be considering all those hapless project managers and toiling masses of IT staff that completed one the biggest, complex and most critical projects in corporate history on time as nothing less than local heroes. However that would be very un-British wouldn't it?

Don't Count your Chickens

As the corporate witch-hunts get underway, spurred on by the media, the Y2K gurus are far from convinced that the worst is over.

Robin Guenier, Head of Taskforce 2000 stated in January;

"It's too early to throw our hats in the air. We are less than halfway through seeing what problems surface but it has been good so far."

Guenier believes that businesses won't be able to breathe corporate sighs of relief until June 2000.

"We have to wait and see what happens. All the problems so far have been minor. The roll over is not the big issue as that can be easily tested. The biggest issue has always been what will happen after it once the daily business practices such as payroll, ordering and invoices start up again".

Peter de Jager agrees claiming that a litany of lawsuits are waiting to happen as companies fix problems as they surface. He adds, ominously, this is not a prediction but a description of what is already taking place.

Christmas Meeting Photo Gallery

Thursday 16 December 1999
London Chapter's Christmas Meeting - a "just for fun" event. Annabel Lane (our very own editor) presented an extremely, tongue in cheek audit report to the "Shareholders" of Greenland Enterprises, proprietor Mr F. Christmas. Annabel would like to thank Andy Farrington for his sterling help in producing the report!

Pictured Right:

Annabel Lane, Audit Elf, Greenland Enterprises.

"Shareholders" enjoying pre-meeting drinks.

Left to right:

Antony Levy, David Thompson, John Mitchell, Alan Brodie and Gerry Penfold

Left to Right:

Charles Mansour, Jean Booth and Bob Oliver.

Left to Right:

Mark Thacker, Gerry Penfold and Karen Nelson

Left to Right:

Jeremy Lewis, Philip Acott and Gabriel Lung

No doubt hapless Y2K project managers, having been vilified in the media for wasting money on a millennial non-event, can expect to be attacked as failures should the next few months prove less than smooth.

Encryption Keys Unsafe

The New Year was ushered in by a report from security company 'nCIPHER'. The report claims to be based upon the first research ever published to prove that encryption keys located on networked servers server can be hacked to decode confidential information.

It was previously thought to be impossible to hack encryption keys from a network because they represent small pieces of code hidden with a mountain of information. Many new entrants to the e-commerce market place have taken to storing encryption keys as software on servers rather than embedding them in the hardware as banks have traditionally done for ATM networks. The research demonstrates how hackers can locate these keys with relative ease - putting the development of e-commerce and on-line transactions at risk.

Neil McEvoy, the MD of Security Consultancy 'Hyperion' has reviewed the report and states that it appears to demonstrate what many in the security sector have suspected for a long time adding that;

> *"In the rush to embrace e-commerce, people forgot the basics of security and have neglected to keep their keys safe. I think that this research is timely and important."*

McEvoy concedes that as producers of hardware based encryption technologies, 'nCIPHER' have a vested interest in the report but goes on to add that the underlying research is quite valid.

Microsoft and SUN/Netscape have also endorsed the findings and commenced work in January to find a solution to the problem.

Hack Attack

The widespread hack attack predicted for the millennial rollover does not appear to have materialised but some organisations had their fair share of problems. The Railtrack web site was hacked over the holiday period and customers were treated to a message declaring that all trains had been cancelled either side of January 1st. Cardiff City Council was faced with amended web pages, which declared that readers were all sheep. The Lloyds of London site was attacked twice, once at 4am on 2nd January and once again on the 3rd at noon. Fortunately all the incidents were corrected within hours.

Lloyds stated that that when the hack was detected, all services were swiftly moved to secure servers and when on to reassure customers and business partners that the organisation' s internal systems are not linked to the Web Site.

Deri Jones of security specialist NTA Monitor declared that the millennium period was 'business as usual' adding that ". There is a level of attack going on all the time, most attacks are low level but from time to time people get hit with a more focused attack. We weren't over surprised'.

Virus Armageddon?

The virus writers like the web site hackers were probably to busy partying over the millennium period to concentrate on 'work'. The holiday period proved to be unusually quiet with the 'Armageddon' predicted by many software vendors failing to materialise. The quiet period was probably aided by a number of companies 'switching off' their email systems over the extended holiday.

Anti virus software vendor SYMANTEC identified 12 new viruses between 27th December and 31st December but the company reports that only three, W95.LoveSong.998, VBS.Tune and Wscript.KakWorm - were found in the corporate environment. However, Alex Shipp, Virus technologist at ISP, Star Internet sees little reason for complacency;

> *"If the virus writers have got their heads screwed on they won't have released their viruses before the millennium - they will have waited until people are back to work. So I think we've got to keep our vigilance up now and make sure that we're still protected."*

E-Commerce/Extranet Practise

By Deri Jones, NTA Monitor Ltd

There are a number of issues to consider when planning to allow external users to access company data systems across the Internet, as part of an Extranet or E-Commerce Project

Internet Perimeter Security issues

1. **Perimeter authentication** - how to ensure that the remote end-user is permitted access through the perimeter. There are a number of different methodologies that can be used here, that may use functionality within a firewall product, or may involve additional authentication systems added to the perimeter.
2. **Encryption of data in transit** - thus is prevent any third party able to 'sniff traffic' in transit from reading the contents. This can be provided at a perimeter level in a firewall or associated system, or alternatively SSL connections from end-users to the web systems can be used - which is a common 'e-commerce' standard.
3. **Location of servers** to be accessed remotely by the external users. The choice here is to pipe connections though the firewall perimeter either direct to an internal server (ie one behind the perimeter altogether, or else to add a new application server on the Firewall 'DMZ' (De Militarized zone - neither on the company inside LAN, nor outside of the perimeter, but within the perimeter) , which collects data by connecting to the Internal systems.

The latter approach is better from a pure security perspective because it limits the damage that can be done in the event of the server being breached, by having it outside the internal corporate LAN. But the former is often the quickest and easiest as the internal server is already in place.

Issues in the Application being used

The application referred to here means the system providing the information to the external user, and typically comprises a web server, a database and some middle ware or bespoke programming linking the two and providing the applications 'look and feel' to the end user.

1. **Replication issues** in the datasystem.

   It is not ideal to allow the external users access to the main internal database via the application, because in the event of a security in the Extranet system there is more scope for the internal database to also be impacted.

   It is better therefore to have a second copy of the database, using replication or some such technology, which the Extranet application can query.

   Typically this database copy is best located on a DMZ in the perimeter.

   If a database copy can not be arranged, then the extranet system will run live queries to the internal database system.

   What are the technical details of the data channel required between two servers for live queries and for replication/copying, and can they be satisfactorily piped through the firewall?

2 **Individual User authenti-cation in the application** - does the application allow individual users to be authenticated (name /password is sufficient where an encrypted channel is already in place from a previous layer in the perimeter security).

   And more importantly does the application ensure that only the right data can be viewed by that user (e.g. customers can only view data for their projects, not that for other customers).

   Does the application have a strong mechanism for storing user names and passwords within the application? (encrypted pass-words - string or weak encryption etc)

3 **User activity logging** - does the application provide sensible levels of logging of user activities - to assist in spotting and preventing misuse - i.e. is there a good audit trail. (Note that logging at the perimeter/ firewall layer also provides useful data but will typically not show what actions the user made within the

application, i.e. what data was viewed or edited etc.)

Can the audit trail within the application be matched to the firewall logs - this requires the use of time-synchronised devices, to match perimeter logs to application user-ID logins using the log-in time as the match. Typically using NTP (Network Time Protocol) to time synchronise the perimeter and application server clocks.

4 **User directory administration** - authentication at the perimeter firewall level and at the application level may be integrated into a single authentication or may be done separately, but either way is there a scalable user directory structure, so that the administration work of adding and maintaining user accounts is not onerous. Some new user directory structure may be required to handle this (e.g. Radius, LDAP or etc).

5. Has the Application had any kind of independent **product security audit** - whether 6-figure cost certification such as ITSEC or Common Criteria - or some other?

6 Can the application vendor demonstrate **other users** who have got the Extranet delivery working in practise and who can share their experiences?

Overall functional issues

1. **Speed issues** - will the application server support multiple concurrent users via the external channel? Does the extra work of rendering data to suit the external users client (whether Web or bespoke) cause significant slow-down? Can the planned end-user system be first bench tested? Using a bandwidth limited connection (not ethernet) to emulate a modem-connected-end-user and a limited Internet pipe at the hoster end?
2. **Reliability/resiliency issues** - what outages can the client accept? How much 'High Availability' elements can be added, and at what cost? Should specific 'High availability' software be used, expensive, versus options for cold-standby spare servers or other options? How much Internet resilience is required - multiple ISP's?
3. **Software to be used by external user** - typically a web browser is the easiest in terms of user familiarity and to allow the supplier to avoid supporting bespoke software at the end-users desk.

This also allows the use of normal Web protocols to be used, which are the least likely to have problems due to filtering at end-user site perimeter.

Special Interest Group (SIG) Fraud Prevention

Rearranged Initial meeting - 24 February 2000

Charterhouse Bank Ltd, 1 Pater Noster Row, St Paul's, London, EC4

ISACA special interest groups meet informally to discuss specific areas of interest to their members and this note is to introduce a new group looking at the subject of Fraud Prevention. At this meeting we'll be setting out the areas the group wants to address. So if this is a topic you're interested in, come along and, as in the famous quote - "..share what you know, learn what you don't".

The topics could include:

- ✦ E-Commerce is often touted as the safest way to buygoods, but is it the riskiest way to sell?
- ✦ What are the characteristics of 'electronic fraud' opportunities?
- ✦ Where do certification and the use of electronic signatures fit in?
- ✦ Common and not-so-common frauds
- ✦ Fraud statistics
- ✦ Detecting and deterring frauds.
- ✦ Supplier & vendor frauds
- ✦ Employee frauds
- ✦ Defences
- ✦ Behavioural risk assessment
- ✦ Money laundering
- ✦ "at risk" business processes
- ✦ E-Commerce

The group would be looking to produce an ISACA publication on this subject. This SIG is suitable for internal and external auditors, IT security and e-commerce specialists from the commercial and financial sectors. (even if you just want to get your name on a publication for your cv!)

For further information contact John Hunter on 01635 248944, or at mailbox@jhunter.u-net.com

Controlling and Auditing Electronic Commerce - Part II

By Keith Osborne

The previous article gave an overview of controls in e-commerce. In this article, Keith Osborne takes a look at abuse and fraud in e-commerce.

5. Abuse and Fraud in e-commerce

All abuse and fraud of information systems, including those that are computerised (which is, of course, now the majority of such systems) is a Business and Management Issue as much as a technical issue. Any abuse and fraud results from some kind of breakdown in control, and computer abuse and fraud should not hide behind technology. It is the realisation that computer abuse and fraud results from not just a breakdown of controls in IT systems, but also the controls associated with, and surrounding those IT systems.

Control failure is either unplanned or deliberate. In the case of unplanned breakdown of control, then the control framework, and the specific controls implemented, were not robust enough for the operation. Deliberate breakdown of control is where has been a concerted effort to override or negate a control framework which, for other circumstances, would be adequate. However, it is right to point out, as already noted, that it is not sufficient to have only controls of the technical infrastructure. There must be business and management controls as well, all controls working with others.

The potential for abuse and fraud in e-commerce is high, because:

- rapid shift of business systems and processes to electronic means
- high dependence on IT assets systems and environments
- speed of IT operations
- complexity of IT operations
- "compartmentalisation" of key skills
- individual business process functions separated and handled by individuals
- lack of individuals having "the big picture"
- vast and continuing increase in the volumes of business information
- pressure on resources available to monitor and control
- new opportunities for fraud for those with specialised IT skills
- effects of new technologies
- pace of change of introduction of new technology
- organisational changes
- culture changes
- control systems have not yet caught up with IT

It is this last point that is particularly important, that Control systems have not yet caught up with IT. While the technology has developed very quickly, control methods have lagged behind, and this has some worrying consequences for trading electronically.

What are some of the characteristics of abuse and fraud of electronic trading? Every case is different of course, but some of the key indicators are:

- conceptually simple
- relies on failure of associated non-IT controls
- discovered some time after perpetration
- discovered by either accident, or "Whistle-blowing" or other tip-off
- well-concealed

Concealment may be by reason of the volume of the transactions, by the complexity of the whole operation (which is a function of the technical infrastructure), the speed with which e-commerce takes place, or for reasons of timeliness (especially with international money transfers and dealing).

There is not space in this article to detail specific types of abuse and fraud of e-commerce systems, but it is nonetheless worthwhile identifying some of the ways in which abuse and fraud can be perpetrated. These are:

- Authority hijacking
- Re-routing
- Timeliness
- Alias techniques
- Cumulative accounting

Again, for reasons of lack of space, it is not possible to give a detailed description of how abuse and fraud in e-commerce can be investigated, other than to summarise some of the techniques:

- Having a clear understanding of the relevant IT Systems and their interfaces

- Having a clear understanding of reconciliation and control processes

- Knowing what the non-IT processes and interfaces are.
- Who the final financial beneficiary of any IT system should be.
- Understanding the areas where control can be firmly enforced, and the areas where control cannot be so firmly enforced.
- Suspicious transactions.
- Prime documents that are unusual, suspicious or false.
- Statistics and trends.
- Unusual or unexpected activity patterns.
- Fraud Profiles and Templates.
- Use of Computer Assisted Audit Techniques.

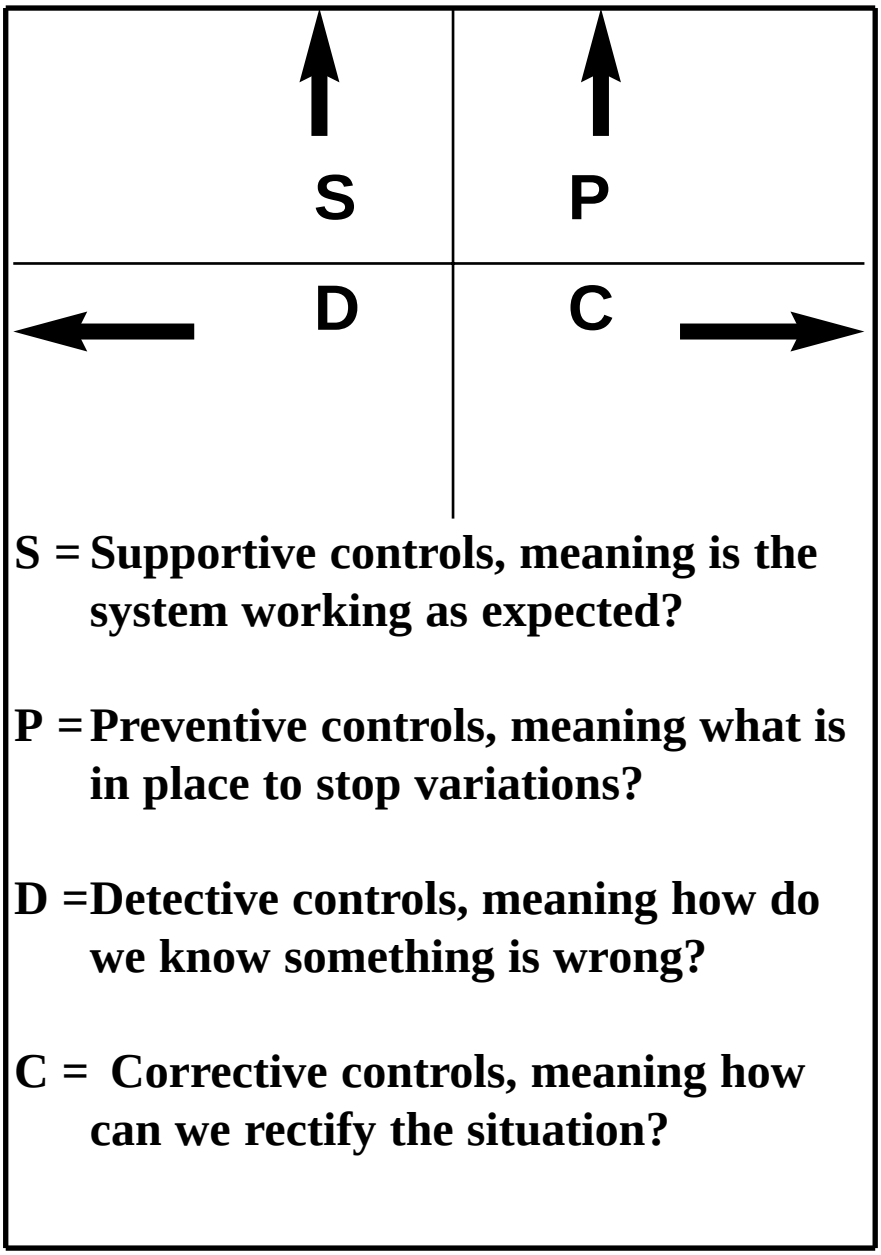
As the emphasis in this article is about control, it is important to understanding that the areas where control can be firmly enforced, as noted above, include:

- control mechanisms internal to the organisation
- organisation's IT assets, systems facilities and environments
- organisation's own staff

and the areas where control cannot be so firmly enforced include:

- trading partners' IT assets, systems facilities and environments
- competitors
- suppliers
- other third parties

A key aspect of investigating e-commerce abuse or fraud is the mapping of control types to fraud types. This is summarised in the diagram above:



Keith Osborne is Principal, Information Security with ICL. He is actively involved in many aspects of commercial Information Security.

His involvement with ISACA has been considerable: he was involved with the EDPAA Northern chapter from the beginning, and was that Chapter's secretary for two terms.

He can be contacted on 0118-935 9751.

Notes :

[1] Technical Infrastructure issues will be looked at in a subsequent article

[2] The terms "Abuse" and "Fraud" (of e-commerce) are used together in this article. The distinction that would be made between them is that abuse of such a system is use of the system for purposes other than intended, and fraud is such abuse with a definite financial objective.

The Security Column

By John Benton

Our regular security guru, John Hunter, is in sunnier climes as we go to print, but John Benton has ably stepped in, focusing on Physical IT Security.

There is nothing new about a database.

It obviously occurred to our ancient ancestors long before they had invented written language, that posterity would be interested in the drawings they carved in caves, thus founding a science called epigraphy, perhaps better known today as graffiti. With the advent of words and the letters to form them the urge to record became almost overwhelming, and the kindred science of palaeography - the study of ancient writings - was born. A further boost was the arrival of paper1 believed to have been first made in China. In the 8th century b.c. the Arabs who had occupied Samarkand were attacked by the Chinese who were beaten off but left behind the secret of paper for the Arabs to adopt and develop into papyrus.

Thus began the avalanche until today we can hardly move for the stuff - and its most greedy customers are the computer, the fax, the photocopier, and the newsprint industry. Electronic recording of data may displace paper in the next century but it is doubtful. Meanwhile alongside mankind's lust for recording is the equally important task of preserving the substance on which the information is written, or printed by mechanical or electronic means.

The restoration and preservation of ancient documents is a fascinating branch of technology calling for great skill and patience. Coupled with it is the treatment of modern paper records damaged by fire or flood.

The importance of records, especially deeds of property, has been taken seriously since the dawn of law-abiding civilisation, but only comparatively recently have specifically fire-resistant containers become available. The "safes" of the Middle Ages were thief resistant chests or coffers but had no insulation. The first patent for fire-proofing was taken out in 1801 by Richard Scott but there is no trace of its use. However in 1834 another was granted to William Marr, followed four years later by Charles Chubb, and in 1840 by Thomas Milner. One of those names is still very much in the record protection business today. Those patents covered the concept of combining thief and fire protection in one enclosure which was fundamentally flawed because the objectives conflicted. Thicker and tougher steel was required to beat drills and gas-cutting tools which did not help fire protection. Several ingenious insulators emerged including Epsom Salts and sawdust which would provide a damp jacket if heated covered by a patent awarded to Edward and John Tann in 1843 which Milner challenged as infringement. Insulation linings today mostly consist of materials such as diatomaceous earth, and we look to the United States later in the 19th century for the origins of purely fire resisting safes and filing-cabinets

Closely associated with this development was, still is, the name of Remington Rand, and it was not before special insulated containers for mechanized ledger cards, punched cards, and index cards appeared. The trend was taken up by European safe-makers in the thirties, the most common product being four-drawer insulated files. These units would give tested protection to paper records for one or two hour periods sometimes coupled with a 30 foot test. Later came the problem of protecting microfilm holding data on celluloid, and all the more valuable for being compressed, like today's computer media which soon followed.

The higher physical sensitivity of these records demanded a new approach to safe construction and insulation. Floppy discs for example are vulnerable to temperatures over 50 degrees Centigrade and there is the danger

of damage by dust or damp and malicious or accidental corruption by the proximity of a magnetic field. Of course computers offer a backup resource but it may not be comprehensive. Some laptop users are notoriously reluctant to download data seen as confidential or just not necessary. For whatever reason, expensive (around £5,000) data cabinets are selling well. Because the market is discerning and sophisticated and the data so vital, independent proof of quality is required and this is now provided by a European Standard - EN 1047-1 published last year. Prior to that German VDMA Standards were a useful yardstick, and there are similar Standards in the U.S.A. established by the Underwriters Laboratories.

Standard EN 1047-1 is entitled "Secure Storage Units Classification and methods of test for resistance to fire1 - Data cabinets". Part 2 on data rooms and data containers is in preparation. . It is a public document obtainable from the British Standards Institution whose Secure Enclosures Committee (Gw2) represents the United Kingdom on the CEN Technical Committee TC263 comprising eighteen nations (EU plus EFTA

The testing conditions simulate fires in order to grade cabinets in accordance with their ability to protect temperature and humidity sensitive contents. Two types of test are carried out; a fire endurance test and a fire shock and impact test. Two time scales are specified viz; 60 minutes and 120 minutes, and three levels of protection; paper documents "D" heat/humidity sensitive media which information below 70 degrees Centigrade; and "DIS'1 for media losing information below 50 degrees (e.g. diskettes) Thus the lowest Protection Class is 560P 1 hour protection for paper and the highest 5120D15 two hours for media of greatest sensitivity

The fire endurance test requires a cabinet to with-stand a furnace temperature of 1049 degrees for 120 mins or 945 degrees for 60 mins. After shutting the furnace down the cabinet is left inside for the cooling or "soak-out" period of at least 1 hour after the peak interior level (measured by irreversible thermocouples) in the case of P grade, and 12 hours for D and DIS grades. The fire shock and impact test requires the empty furnace to be pre-heated to 1090 degrees before inserting the cabinet with only 4 mins. allowed for the door to be open. The heat must then resume at 1090 degrees within 15 minutes and be maintained for 22.5 minutes for 560P/560D/560D15 or 45 minutes for 5120/P/5120D/5120D15. Following this heat must be shut down and the cabinet be removed for a drop test from a height of nine metres on to a prepared bed of pebbles on a base of concrete at least 300 metres thick. Thereafter it is replaced in the furnace to be reheated for the same periods as above and remain throughout the same cooling period(s) as for the fire endurance tests. Obviously after all these trials the information must be unimpaired otherwise it is a failure

The EN1047-1 Standard does not contain any reference to testing and grading in respect of corruption of data held on the media as a result of possible electro-magnetic interference although most manufacturers claim such properties for their products. The whole subject of intended or accidental radiation which may compromise data is dealt with by the Government Communications Electronics Security Group based at Cheltenham. They offer services and advice on counter measures on the problem designated TEMPEST including training testers and on-site qualification of operational systems. Their remit extends to many forms of data security and they are most anxious to help, starting with a Seminar later this year. Contact Mr. Martin Purches Room 2/6069, P0 Box 144, Cheltenham GL52 SUE.

Data Rooms are an extension of the Data Cabinet concept and will shortly be the subject of Standard EN 1047 Part 2. They are costly up to £lm) but their cost is usually only a fraction of the value of the their contents. They are increasingly being installed by governments and very large corporations who

The data is the target and executives are stalked like marked men.

Continued on page 24.

Career 2000?

By Adrian Simpson BSc ACA FIIA

Well, I hope we have made it! Articles written before, but published after the start of the new millennium, carry a rather greater risk than usual of the author being caught out by events.

The Y2K problem should by now be substantially resolved and we can proceed as before.

1999 was not a good year for computer auditors. The cause was the run down in Y2K work and the unforeseen but logical postponement of large numbers of new developments and initiatives until after the millennium. There was more unemployment amongst computer auditors - and particularly contract staff - in the latter half of 1999, than I have seen before. Matters should improve significantly during this year - although it is not all unalloyed good news.

The greatest risk to the employment of computer auditors is probably that of a profitless future. If you look at many sectors of the economy, companies are finding it difficult to increase or even maintain their profitability. Regulation in the utilities sector is driving prices and profits down. Many areas of the financial services industry together with virtually all of the retailing, transport and distribution sectors, are facing unprecedented competition. Volumes may be up, but prices are down. Manufacturing is now living with an exchange rate that as little as a year ago was supposed to make many exports unprofitable. E-commerce is only encouraging this competition. As a consequence consumer price inflation is for the moment dead. The effect of this is that companies are ruthlessly reviewing their cost base as they strive for greater efficiency. As a cost, computer auditing is there for all to see and needs to justify itself.

1999 was not a good year for computer auditors

In year 2000 never will the adage "no I.T., no business" seem more appropriate.

The good news? First, many companies now have a backlog of new systems developments, both bespoke and packaged, that will follow a conventional life cycle and require traditional audit input. Demand will continue for core infrastructure skills such as datacentre, disaster recovery and change control where technical platforms are becoming more consistent. Client server environments have become firmly established and despite many predictions to the contrary, large mainframe computers will continue to feature. However, e-commerce initiatives are going to multiply and are likely to change the emphasis away from conventional system development life cycles to a more rapid and flexible approach. Business critical applications will be developed in as little as six to eight weeks. For those computer auditors with the skills and experience, e-commerce is going to be a huge growth area. Specific knowledge of networks, firewalls and web architecture will increase your marketability.

The second piece of good news is that towards the end of last year the Turnbull report was issued. This is the latest and, for internal auditors, the most important step in a corporate governance process that has lasted almost ten years. As executive management address the risk management and internal control issues necessary to implement Turnbull they are going to need internal and computer auditors in a way that they have never needed them before. It is perhaps ironic that while developments such as e-commerce place a greater emphasis on the need for technical skills, the now all encompassing nature of I.T.

requires computer auditors who appreciate a wider picture. Computer auditing will still be about understanding the technical issues; it is essentially a technical discipline. But to be effective, computer auditors will need to know much more than this. They will need to understand business, they will need to understand risk and they will need to understand internal control.

An obvious impact of this will be in the training and development of computer auditors. Traditionally computer auditors have taken a large share of the training budget to keep up to date with emerging technologies. The increasing requirement for computer auditors to have business knowledge will add to this cost. Unlike general audit, computer audit skills have historically been readily transferable between business sectors. It is more likely that employers will in future wish to recruit computer auditors with relevant sector experience.

Many computer auditors have benefited from the flexibility and freedom that contract work has offered. Cost pressures and the need to buy in bespoke skills when needed is likely to stimulate the demand for contract computer auditors. A market that was very slow during 1999 is likely to grow significantly during 2000. In year 2000 never will the adage "no I.T., no business" seem more appropriate. It should be a good year to be a computer auditor.

Adrian Simpson is director of Barclay Simpson, a Consultancy specialising in the recruitment of Internal and External Auditors.

Continued from page 22

originally sought security for data by down-loading at regular intervals to remote locations as a precaution against disaster at the centre. But however frequently downloading is done, some data will remain at risk. Moreover downloading is not cheap and transmission is vulnerable. The eggs therefore are considered safer in one central basket - but that basket must anticipate all risks Air conditioning, humidity control, fire suppression, strict access control with audit trails, alarms etc. are essential.

On a more common but equally serious level is the theft of hardware. The losses of PCs and chips have declined some-what from the peak of three or four years ago when insurers were paying out a haemorrhage of claims and a host of locks and anchoring devices were conceived in garden sheds. Under pressure from the insurance companies who largely fund it) the Loss Prevention Council produced Standard No. 1214 and began testing in 1996. LPS 1214 has two security categories viz: (I prevention of removal and (II) access to the outer casing. It is wise to buy LPS Approved equipment if only to keep your insurer happy.

Finally there is the laptop. The most common computer crime is removal of laptops left on the seats of cars, planes, and trains. Mugging commuters in leafy suburban station car parks is a frequent occurrence - especially if the laptop is carried in an obvious bag. 98% of such crime is aimed at stealing the laptop itself - to be disposed of in a pub for a few pounds - or swapped for a dose of crack.

The remaining 2% is more sinister. The data is the target and executives are stalked like marked men. There are systems of emergency erasure of data, and tracking stolen laptops, but all too often trouble is caused by a lack of simple discipline. Company laptops should be numbered and registered as the responsibility of a named executive. Removals from the office should be authorised by the CEO and recorded. Devices of the anti-shoplifting type are available to raise an alarm in the event of unauthorised removal. They may not be 100% proof (what is?), against smuggling machines out and back but at least they serve to underline a serious view on the part of senior management. The laptop is a useful - perhaps essential - tool but it should be regarded as a burden not a status symbol.

John Benton obtained Management and Security training with Chubbs, ultimately becoming responsible for Western Hemisphere business. He left for wider horizons but was swiftly head-hunted back into security to become Managing Director of John Tann Ltd for twenty years, during which Tann became an international Group.

He took up consultancy after retiring early in 1985 and was a founder and first Chairman of the Association of Security Consultants, remaining a Director.

John is Chairman of the British Standards Institution Committee on Secure Enclosures, a Member of the American Society of Industrial Security, a Fellow of the Institute of Directors and was made a Freeman of the City of London for services to Financial Institutions. From time to time he writes and speaks on physical security technology.

He can be contacted on:

Tel: 0181 904 8635 or
0181 908 3749

Fax: 0181 908 3749

Central News

By Michael Hughes, President, Central UK Chapter

Welcome to what will be a regular column from the Central Chapter President.

I was elected as President at our AGM in May, after serving my time as Secretary and Vice President. I was instrumental in setting up the Chapter some six years ago and during this time I am happy to say that the membership has grow from 25 to the present compliment of 111. I would like to take this opportunity of thanking my two predecessors Lawrence Devlin and James Whittaker, who have led the Chapter during our first six years and their careful stewardship has left the Chapter in good shape, giving me a sound foundation from where to continue their good work.

I have just had the pleasure of attending my first Area 3 President's Council Meeting (PCM). I was really looking forward to my first meeting, Lawrence and James had been to far flung places such as South Africa, Madrid, Frankfurt, and Denver. I was filled with anticipation when I heard that my first PCM was approaching, where would my first meeting be, Paris, Amsterdam, Geneva? I was overjoyed when I learnt that my first meeting would be in Manchester in November !! On a serious note, the event was extremely well organised, so thanks to Ray Butler and the other members of the Northern Chapter Committee, and it was good to meet the presidents from the rest of Area 3's chapters.

After the main business of the PCM was over, the three UK Chapter Presidents got together to have our own mini UK PCM. We have set the foundations to work more closely together in the future, the first demonstration of this co-operation being this and the Northern President's columns. We are distributing each others Events Cards and full members of all three Chapters can attend each others evening events free of charge. We are also planning to hold a joint one day conference, probably in Autumn 2000. I am pleased to report that it looks like we will soon be joined by a fourth UK Chapter. Organisation is at an advance stage in setting up a Scottish Chapter and the three existing UK Chapters are providing assistance as required.

During 1999 the Central Chapter has had a successful events programme with some very interesting presentations covering a number of topics including: Project Assurance, IT Development Disasters, Year 2000 Contingency planning, Internet Security and PKI. We also recently held a one day conference on the hot topic of electronic commerce and electronic business. The five speakers covered a number of areas of this subject from the business drivers, business issues, the commercial benefits, to the risk, legal, security and control issues. We received very positive feedback from all who attended, if there is sufficient interest we may repeat the conference early in the new year. If you haven't as yet attended an event, you don't know what you are missing!!

I would like to take this opportunity to thank all the speakers who have given their time to come to present to the Chapter throughout the year. Thanks to KPMG, who continue to provide valuable support to the Chapter, providing the facilities and venue for the majority of our events and also to Arthur Andersen who also provide the Chapter with a meeting venue. Sincere thanks go to my committee colleagues and to all the other individuals who work so hard behind the scenes throughout the year, to bring you the members an interesting range of events and keep the Chapter running smoothly. I would like to especially thank Pat McMullen and Michael Farley who perform a wonderful job and vitally important role of managing the administration of the Chapter. Special thanks goes to Oli Ralph, who has performed a marvellous job of setting up the Chapter's Web site, and keeping it up to date. If you haven't visited the site yet, it can be found at www.isaca.org.uk/central.

Oli is presently working on a members' only page, where we are hoping to provide more value for

your membership. We are hoping to use this area for the membership to share knowledge. For this to be successful, we are reliant on the members to submit articles, work programmes, hints/tips etc. So get writing.

Congratulations to those of you who successfully passed the CISA exam this year. In the six years that we have had a test centre in Birmingham, we have had 153 individuals sitting the exam, with 126 passes giving a 82.4% pass rate, substantially higher then the 50% world wide pass rate. Of the 111 current members of the Central UK chapter, 65 presently hold the CISA designation, representing 58.5% of our membership. So come on the other 41.5%, get your applications in to sit the exam next June. The CISA designation is recognised world wide, and it does help if you can include it on your CV !!

I'm sorry, but it is that time of year again when your membership renewals are due and for those of you who are CISAs, to confirm your continuous education. As usual you should send your remittance directly to International HQ in the States, they then send the Chapter our portion of your dues at a later date. Don't forget to submit your CISA CPE details to ensure you maintain your designation. If you are selected to provide supporting documentation to your CISA return, then please do so promptly to ensure your designation isn't revoked.

This year's programme of events has been arranged and details can be found on page 27 or on our web site. We try to arrange events which will be of interest to our members and to keep you up to date on emerging issues and hot topics. However, we need continuous feedback from you, to let me and the committee know that we are putting on the events that you want and in the format that you want. So please let me have any comments you may have.

We are planning to hold a post millennium blues dinner sometime in the Spring. This is to celebrate the passing of the Millennium, hopefully with experiencing few disasters. Watch this space for further details.

With the Year 2000 issue over, what are we going to find to do??

Well there are one or two things that we can get our teeth into:

- ✦ e-commerce/e-business;
- ✦ corporate governance;
- ✦ raising awareness of IT risk management issues;
- ✦ EMU.

....and that's just for starters.

Who knows how EMU will impact on our organisations, watch this space. The other topics though will keep us extremely busy over the next twelve months. The corporate governance issue, and the reporting requirements of the Turnbull report, will give us all the opportunity to take IT governance issues to the 'top table', and perhaps for the first time to get the Board to put IT risk management firmly on their agenda. With the amount of change on the horizon which will have a major impact on how organisations do business and how they integrate IT into the business, the Board need to be aware of IT risk and take a proactive roll to effectively manage this risk. We all need to take an active roll of bringing these issues to the attention of the Board and we are best placed to help the Board manage these risks.

One of the main areas of risk over the next twelve months will be in the area of e-commerce and e-business, where virtually all organisations are going to be looking to do something with this technology. This is going to be a major area of growth in the next few years as highlighted by information gathered by Forrester Research in 1998:

- ✦ 92% of Britain's businesses have access to the Internet or external e-mail;
- ✦ by 2000, 30 million people will have access to the Internet in the UK;
- ✦ 11% of the US population bought a product or service on-line within the last 30 days;
- ✦ US consumers spent over $8.2 billion on on-line retail purchases over the 1998 Christmas period;
- ✦ business to business electronic commerce will grow from $43bn in 1999 to $1,331bn in 2003.

We need to take a proactive roll from the start of an e-commerce project to ensure that our organisations fully exploit the technology to gain competitive advantage or improve customer service and efficiency, but in a manner where risk is being effectively managed. Therefore the challenge facing us all is to:

- ✦ Understand the business drivers and business risks. Ensure that our organisation is not just adopting a 'me too' strategy.
- ✦ Identify the assurance risks and how these differ from more traditional transaction methods.
- ✦ Contribute to channel and product development - can you provide proactive advice on risks and controls?
- ✦ Obtain the business and technical expertise to be able to conduct an e-commerce review, covering both the business issues and the technical control and security issues.
- ✦ Identify what YOU need to do to develop your skills further.

They say that nothing in life is guaranteed accept death, but I can guarantee you an extremely interesting and challenging twelve months ahead, so get in front of your Boards and spread the word!!

Central Chapter Programme of Events 1999-2000

27 January 2000
Data Protection and Legal Issues

30 March 2000 - Gary Hardy
Cobit III

April 2000
Post Millennium Blues Dinner

25 May 2000
AGM/Penetration Testing

14 July 2000
End User Computing

22 September 2000
Business Continuity Planning

We extend a warm invitation to ISACA members of other chapters who find themselves in the area and would like to come along to any of the meetings

Northern Chapter Programme of Events 1999-2000

26 January 2000
Enterprise-Wide Security Management
Leeds

23 February 2000
IT and the Law
Manchester

22 March 2000
CAATs Conference
Salford

19 April 2000
COBIT (As audit tool)
Bradford

May 2000
Internet - Control issues and Audit Methods
2 day seminar
Salford

28 June 2000
AGM and Running a Computer Crime Unit
Chester

EXPERTS SOUGHT!

The Research Board have requested that London Chapter seek out their members for "subject matter experts" in technical areas. All areas are encouraged, but the following areas are especially sought: VPN, Oracle, PeopleSoft, Wireless and Customer Relationship Management.

If you feel you have something to offer, then please get in touch with Nancy, Isacalondn@aol.com

DIGITAL SIGNATURES SECURITY AND CONTROLS MONOGRAPH

This new research publication addresses the technical, audit and control, legal and standards issues related to digital signatures technology. It includes a suggested audit work program utilising the COBIT framework.

The project was sponsored by ISACF, the London Chapter of ISACA and S.W.I.F.T. It can be ordered through the ISACA bookstore at bookstore@isaca.org (US$35 for members, US$50 for non-members).

STANDARDS REPORT

Four new IS auditing guidelines were enclosed with Volume VI of the *Journal: Audit Considerations for* irregularities (replaces SISAS 8); *Audit Sampling; Effect of Involvement in the Development, Acquisition, implementation or Maintenance Process on the Auditor's Independence* (replaces SISAS 2);and *Effect of Pervasive IS Controls.* They are effective 1 March 2000. On that same date, SISAS 2 and 8 will be withdrawn.

Millennium Bug stories from around the World!!

Toronto, Canada: Senior Citizen crime wave!

The crime reporter on a local newspaper thought he had hit on a frightening new trend when his regular review of the local police arrests revealed an apparent crime wave amongst the over 80s, such as an 80 year old man accused of sexually assaulting an 83 year old woman just after midnight on January 1st, and two missing "youths" listed as being 83 and 84 years of age.

A Y2K computer glitch had caused police software to read 2000 as 1900 and the suspects date of birth as their ages. It was fixed the following Monday morning, and the senior citizen crime wave came to an end!

New York, USA: Most expensive video rental ever?

A customer at the Super Video Store in Colonie, New York got a shock on New Year's Day when he was charged $91,250 for returning a video a day late. The owner, unperturbed, cancelled the charge, wished him a happy new year and gave the customer a free video rental. He had, he said, stayed up till 0130 on New Year's Eve running tests to make sure his computer system was Y2k compliant, but hundreds of his customers still faced six figure charges for video rentals.

Cologne, Germany: Banking records nicht in Ordnung

According to a German news agency, an on line customer of a Cologne-based savings bank got a very pleasant surprise when he logged on to his bank account to check the balance on New Year's Day. It was standing at 3,930,129,930 in an unspecified currency.

A 43 year old customer of the same bank found that nearly 13 million Marks had been erroneously credited to his account. It is not reported whether the bank apologised or offered to let the customers keep the funds as the mistake was on its part. But I have a pretty shrewd idea.

South China: First reported malicious virus attack of 2000?

The South China Morning Post reported on January 6th that the virus known as W32.Mypics.Worm had attacked a firm's computer system and destroyed its Bios input-output system. According to the Productivity Council's IT division General Manager the computer is "as good as dead" and data cannot be readily retrieved. 13 other Y2K incidents have been recorded in addition to the virus attack, three of which were serious with one system failure and two software programs that would not function properly.

Washington, USA: Red faces re Fire Department Pay Cheques

When workers at the District of Columbia Fire Department booted up their payroll computer on January 4th, they were dismayed to find it displaying the year as 1900 - one of several city government computers to skip back 100 years when the date rolled over. Capt Richard Sterne of Engine Co 18 voiced the concerns of the employees when he said "They were saying everything was Y2k compliant and then we saw this! What we're concerned about is….are the checks going to say 1900? Is it going to work?" Get those cheques cashed Capt Sterne as banks only honour them for 6 months after the date……