ISSN 1356-0735

AWARD WINNING

DATAWATCH

VOL. 46, OCT-DEC 2000

E-COMMERCE - THE LEGAL ASPECTS

IN THIS ISSUE:

E-CORPORATION AND THE LAW

ELECTRONIC ORIGINAL INITIATIVE

THE QUARTERLY MAGAZINE OF ISACA LONDON CHAPTER

VOLUME 46 OCT-DEC 2000

DATAWATCH

is a quarterly magazine published by the

Information Systems Audit and Control Association

London Chapter

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 2000/2001

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
0207 893 2671
Archie.Watt@bdo.co.uk

SECRETARY
Charles Mansour
The Woolwich
0208 298 5646
Charles.Mansour@woolwich.co.uk

MEMBERSHIP
Kamal Khan
Sanwa Bank Ltd
0207 330 5522
kamal.khan@sanwabank.co.uk

PUBLICATIONS
Annabel Lane
Nestle UK Ltd
0208 667 6530
Annabel.Lane@uk.nestle.com

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

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

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

EVENTS
Karen Sharpe
Deloitte & Touche
0207 303 7478
karen.sharpe@deloitte.co.uk

CISA CO-ORDINATOR
David Spaven
KPMG
0207 311 5620
David.Spaven@kpmg.co.uk

PAST PRESIDENT
Gerry Penfold
KPMG
0207 311 8489
Gerry.Penfold@kpmg.co.uk

WEBMASTER
Allan Boardman
Internet Working 4U
01732 462 133
allan@internetworking4u.co.uk

CISA REVIEW COURSE
Michael Christodoulides
District Audit
01438 351570
m-christodoulides@district-audit.gov.uk

STANDARDS
Joseph Wright
HSBC
0207 771 5369
joe-wright@supanet.com

CHAPTER OFFICE
Nancy Watt
Tel/Fax: 01487 815705
nancy@isaca.org.uk
WWW.ISACA.ORG.UK/LONDON

ISACA Northern UK Committee (officers only)

PRESIDENT
Ray Butler
HM Customs & Excise
0161 827 0875
ray.butler@hmce.gov.uk

VICE PRESIDENT
Robert Newbould
Corus plc
Bob.Newbould@corusgroup.com

TREASURER
Ian Simpson
Halifax plc
IanDSimpson@halifax.co.uk

SECRETARY
Peter Thompson
peter.thompson@deloitte.co.uk

MEMBERSHIP
Alan Rainford
Axa Insurance
01253 662782
alan.rainford@axa-insurance.co.uk

CISA CO-ORDINATOR
Gan Ssubramaniam
Skipton Building Society
gsubramaniam@skipton.co.uk

ACADEMIC RELATIONS
Mike O'Hara
University of Salford
0161 295 5665
m.j.ohara@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
Chris Chandler
Arthur Andersen
0121 233 2101

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

By Annabel Lane

Welcome to Edition 46 of Datawatch, which as you will have seen, once again deals with the issues surrounding e-commerce and our role as auditors in them, but this time with a twist to bring in the angle of legal aspects. I am sure that the articles you'll find within this edition's pages to be useful. I for one am often being consulted on legal aspects concerning e-commerce projects and have found myself at a bit of a loss to make any contribution apart from referring the enquirer on to the company legal department. But with legal cases in this area breaking new ground and fresh precedents being set all the time, it's very difficult for anyone not regularly involved to keep a breast of the issues. The widest ranging of our articles is the one on the E-corporation and the Law, by Andy Farrington, in which he explores some of the legal questions, such as how binding is a contract made via a web site? How binding are digital signatures? We may never become experts in these areas but there are certainly issues of which we need to be aware, especially if asked to advise on new projects in the e-commerce field. Amongst our regular features this month, John Hunter's article also majors on e-commerce and security vulnerabilities and talks about some of the newer tools those nasty hackers are using out there.

The Chapter web site is as ever an area of interest to our members, and our web master, Allan Boardman gives us an update in this issue as to what he has been doing to continually improve services by this route. His comments are actually in response to a member's letter, itself in response to a comment made in the last edition's Editor's Chair column. Feedback from members is always welcome on any of the services we provide, and as you'll see from Allan's reply, we do take all views into consideration. We hope that you will regularly visit the Chapter's web sites and let us know what you think of what we are doing.

Finally, on behalf of the editorial team, I'd like to extend a welcome to those of you reading this magazine because you have passed the CISA exam this year. Congratulations on your achievement, and we hope that you won't just turn to the CISA report to see your names in print, but will take a look at Datawatch and hopefully wish to receive it again. Don't forget; feel free to send in any news and views to me, or any member of the editorial committee.

London Chapter Programme of Events - 2000/2001

For the first time in 1999 we provided a programme based on a theme. The theme selected was "The Extended Enterprise" and, if increased attendance at ISACA events is to be relied upon, it was very successful. The London Chapter Board has therefore decided to continue the themed approach for the monthly meetings in 2000.

Two current "hot topics" pertinent to those of us who work in the IT audit and security profession are governance and e-Business. These issues currently dominate the business world and are becoming increasingly important for not-for-profit and government organisations. Our programme for 2000 has therefore been developed to keep ISACA members up to date with information on changing risks and the "new" approach to managing these risks. Under the umbrella theme of "IT Governance in the e-economy" we will be exploring the impact of the brave new e-world on our organisations and also on ourselves as professionals.

16 November 2000
Will the e-economy change strategic risks in my organisation?
Malcolm McCaig, Deloitte & Touche

7 December 2000
E-Business Availability
Stewart Roby, KPMG

18 January 2001
Controlling the e-developments
Charles Mansour, The Woolwich plc

15 February 2001
Applications to meet the e-need - what are the risks?
Karen Sharpe, Deloitte & Touche

15 March 2001
Forensics in an e-world, or "Who's been hacking my e-business?"
Tad Dippel, KPMG

19 April 2001
Securing the systems - what's new?
Yag Kanani, Deloitte & Touche

17 May 2001
The end of "the audit" as we know it?
Gerry Penfold, KPMG

21 June 2001
Required competencies for the IT auditor in the e-business world
Sarah Blackburn, Lex services

The venues for these meetings will be announced in the monthly Mailshot, or visit the website(www.isaca.org.uk) for information and to make a booking.

From the President

By John Mitchell

Even if you do not work for a listed company you should certainly be aware of the impact of the Turnbull report and the London Stock Exchange on listed company reporting requirements for the current reporting year. Where listed companies go, the not for profit and smaller companies will almost certainly follow which is why this year our theme is corporate governance.

The management of Information Technology is a component of the overall governance process and as such should fit within the general governance framework. In simplistic terms IT management must have a demonstrable process in place to show how they have identified risks, how they have managed those risks and how they have reported key residual risks to senior company management. Internal Audit needs to review this mechanism for completeness and reliability. There are both direct and indirect ways of doing this and I suspect that most of you plan to do both. Directly, by reviewing the actual process and indirectly by auditing some of the key risk areas to see whether you end up with the same results as IT management regarding the management of individual risks.

Another indirect way is to initially assess the reliability of the local control environment. Are policies, standards and procedures being adequately communicated to staff? Are staff following those procedures? Are the procedures regularly reviewed to take account for changes in the business and technical environment? If you get a warm feeling on the general control environment, then you can be more relaxed in relying on management's representations on risk. This can be reflected in your audit approach and you can make more use of Control Self Assessment. coupled with attestation and confirmation reviews to reduce your direct audit activity accordingly. Broader coverage, but less depth.

If however, you conclude that the general control environment is weak you will need to do more direct audits, because you are unable to rely on management's assertions regarding risk management, or anything else for that matter. The situation you really want to avoid is being at year end and reporting to senior management that they can place no reliance on IT management's representations on risk management.

At best this begs the question as to why you did not raise the point during the year so that remedial action could be taken.

At worse it means that your company is not in compliance with Turnbull. Not a good thing either way if you are a listed company. So the message is clear. Cut your audit cloth to fit the IT body.

Happy planning.

Mind Games
by Puzz

The answer to each clue is a word which links with each of the three words listed. This word may come at the beginning (e.g. ODD linked with BALL, FELLOW and SOCKS), at the end (e.g VILLA linked with ROMAN, ASTON and HOLIDAY), or a mixture of the two (e.g. AGE linked with BOND, BRONZE and GAP).

Once you have solved all the clues, take the first letter of each word and rearrange them to form a word well-known to us all. Answers on page 20.

1. ICE	END	SET	.....	**5.** WHEEL	RIDGE	APPLE	.....	**9.** BIRTH	BLACK	TIME	.....
2. OVEN	BOARD	MICRO	.....	**6.** GENERAL	CHAIR	FENCE	.....				
3. BEER	SQUARE	TAP	.....	**7.** WHITE	GRASS	PINK	.....				
4. PENNY	BAGS	BOX	.....	**8.** CLOSING	BIRD	DAYS	.....				

The 'E-Corporation' and the Law

By Andy Farrington, CISA

This is the first part of an article on e-commerce and the law. The second part will be published in Datawatch Issue 47.

I am writing this article in August 2000 and the press reports of security breaches and failures that have affected a number of Websites, particularly in the financial services industry, are still the subject of interest in the Media. As IT auditors we are all in the business of doing what we can to prevent our respective employers from scoring 'own goals.' We can all read the press reports and we can all become animated about load and stress testing, the adequacy of security, penetration tests, intrusion detection, resilience and the scalability of the architecture to meet demand. The fact is, however, that the 'technical' matters are not the only ones with which we should be concerned.

It is now almost a cliché to say that e-commerce has done away with geography. While we can expect continued rationalisation of the weaker e-commerce propositions a number of others, particularly in the B2B market, have the potential to provoke radical transformations in the way in which business is conducted. Many of the new companies emerging are 'born global' by virtue of delivering goods and services via a Website. Fortune magazine in the US has coined the term 'e-corporations' to describe such businesses Companies such as Amazon.com have emerged from nowhere to become a global player in the supply of books, services and music without having a physical shopfront anywhere in the world. For such companies the nature of the Internet and the ease with which Virtual Private Networks can be established using tunnelling technologies mean that procurement and delivery systems can span several continents while still remaining part of a virtual whole. In such circumstances legal jurisdiction becomes an issue and it is the manner in which this relates to the 'e-corporation' that is the focus of this article.

As auditors we are not legal specialists and we would not seek to usurp the responsibilities of the corporate legal department. Our main role is to identify and seek out the means to control risk. In e-commerce developments, risk is not limited to the technology but extends to the legal environment in which it will exist. Project managers are rarely legal experts and in some organisations the corporate legal department may not stand as close to e-commerce developments as they should. To be effective in adding value auditors must have a sufficient understanding of the legal framework surrounding the Internet environment to at least identify when specialist legal advice is required. This article is intended to provide some general guidance, based upon my own experience. I intend to cover the issues of contract formation, Web Site terms and conditions statements, digital signatures, copyright and trademarks, domain names, hypertext linking, metatags, privacy and data protection, cross border data flows, the legality of 'cookies', defamation and the legal admissibility of electronic evidence. Wherever possible I will endeavour to provide an international perspective as well as details the latest case law (applicable only at the time of writing - this is a dynamic area!) on the issues both in the UK and abroad. I will be using the financial services industry as an example mainly because it is the industry with which I am most familiar but the use of a specific as an example does not discount the general principles raised which are equally applicable to other industries.

In considering the application of the law it is important to understand the following principles.

Most Law and regulation is territorial

With the exception of certain international agreements and conventions, laws and regulators are territorial. The enactment of law is only as good as the system of enforcement put in place by a Nation State. The laws, which an individual must abide by, and the sanctions that apply should those laws be broken depend upon the geographical location of the individual.

By contrast, the Internet (as mentioned above) is global. A Web site built in the UK must comply with the framework of law and regulation in the UK. However, by virtue of the fact that the UK Web site is accessible to any citizen anywhere in the world equipped with a PC, browser and an Internet connection, it is global in nature.

This generates issues which have not been considered before by legislators. What if the products sold on the Web site are regulated in Armenia? Could the owner of the site be subject to legal action from Armenia because the Web site (and by inference the product) is available to Armenian citizens. What if the trademark, appearing on the site, lawfully registered in the UK, conflicts with a trademark lawfully registered by an Armenian company in the same line of business? Could the owner of the site be subject to litigation for an 'infringing' trademark available in Armenia?

'Cyberspace', to use the phrase first coined by William Gibson, is not a 'territory' that can be easily regulated. Litigation associated with the issues mentioned above is becoming more commonplace due the ubiquity of the WWW and the speed with which companies are developing an 'on-line' presence.

Law, regulation and technology have not kept pace.

The passage of law and regulation into the public arena is subject to the protocols of the legislative process within each country. Making law is a time consuming process involving considerable amounts of debate and consultation. Establishing a global legislative framework to regulate the Internet is even more time consuming as the consultation process must involve each country which will be subject to the law, each of which has its own agenda and rights of veto.

The growth of technological innovation is, by contrast, very rapid particularly in the case of e-business which is driven by the need to retain market share, reduce costs, improve business processes and customer relationships or seize global marketing opportunities that may not previously have been viable.

As a result, the law and regulatory framework lags behind the technology. This is a major problem as in many respects the law is an important enabling factor for the growth of e-business.

Laws must be Interpreted

Finally, even if foresighted legislation has been passed, it can rarely anticipate every eventuality. The application of law in particular circumstances needs to be clarified. In many countries (the UK is a good example) clarification depends upon a body of case law to set legal precedents. Much e-commerce enabling legislation around the World is generally too new to have a reliable body of supporting case law.

CONTRACTS

The Internet is at root a delivery channel either to customers or to other organisations with which we do business. Many of the relationships arising from this delivery channel are contractual in nature: in the case of a bank for example, the exchange of financial services or products for money. This means that it is important to, understand, when we are communicating electronically, with whom we are contracting, the laws which are applicable to the contract and when a contract can be said to have arisen.

The precise nature of contract law will vary from country to country but the general principles are similar. Using the UK as an example, there are four principles:

- an offer must be made by one party
- an offer must be accepted by another party (an acceptance subject to alterations is legally regarded as a 'counter offer' and is therefore still an offer).
- there is an intention on the part of both parties, to create a legal relationship
- there is consideration (i.e. something of value such as money, services or goods passes between the parties).

Provided that these criteria can be shown, a contract is regarded by the law as having been formed when the offer was accepted.

In circumstances where the other party is not physically present and where there is no physical exchange of signed documents a number of issues need to be taken into account. *These issues are not unique to contractual relationships using the Web they are also applicable to other delivery channels such as the telephone and as such they are clearly not insoluble. It is, however, important to understand them in the context of the Internet.*

With whom are we contracting?

Taking banking as an example, if we meet a customer face to face over the counter of a branch we can gain a lot of information about the customer such as their age and their mental capacity and it is relatively easy to request further information, such as their date of birth or other identifying characteristics. These can be checked. We also know the location of the customer at the time of the contract.

Banks, however, are regulated institutions and when we are conducting transactions on a virtual basis over the Internet, (or over the telephone), important information is denied to us for example:

- is the client who they say they are or could they be a fraudster?
- is the client a money launderer?
- is the client old enough to contract with us? and
- is the client a resident of the UK?

Similar concerns are likely to exist in other countries as most have regulations or legislation covering these areas. The Money Laundering Regulations in the UK date back to 1993 and were put in place before the growth of e-commerce. These regulations apply to any 'one off' transactions over the £10,000 limit, (or in the case of the EU, 15,000 ECU) They place an obligation upon licensed deposit takers, such as banks to obtain satisfactory evidence of a customer's identity thereby constraining the extent to which sole reliance can be placed upon an Internet message. Compliance with this legislation is still a requirement despite the fact that delivery channels have changed. This raises some interesting issues in the potential for using automation and internet routing technologies to break a large sum into a series of micro payments, differentially routed through the global financial system to eventually arrive at the same account. Would this be detected?

Both the Financial Services Authority (FSA) in the UK and The Securities and Exchange Commission (SEC) in the USA have stated that they will take action against foreign based financial service providers if material offending *their own financial services regulation is accessible by, respectively, UK and US citizens*. Clause 19 of the new Financial Services Act in the UK requires that promotional material directed at the UK can only be disseminated by FSA authorised firms. It is likely that other national regulators will adopt a similar stance as the regulation is based upon the recommendations of the International Organisation of Securities Commissions (IOSCO) Internet task force. Forming a contract with a non-UK resident for a product or service which offends the regulatory regime of their host state could place a bank in an embarrassing position and could lead to regulatory censure.

Under what laws are we contracting?

The global nature of Internet communications means that a Web Server based in say, the US could serve customers in the UK or other EU states. Because the enforcement of contract law is territorial it is necessary to be clear about which territorial contract laws govern the formation of contracts i.e. where does the processing take place. There are several factors which may need to be taken into account including the issue of which country within the contract routing process 'owns the Web site' as well as the territorial location of the hardware. However reaching a definitive view may not be easy. The information that gives rise to the contract may reside on a few files spinning on a disc in the USA. However, what if the 'e-corporation' has several 'mirror sites' around the world, any one of which could be used as the basis for the transaction between the buyer and seller to occur? Mirror sites may well be used as the basis to improve response times for customers. To confuse matters further, the sellers web site may be Java enabled. This means that it will load programmes called 'applets' on demand from the seller's site to the buyer's computer. This raises an interesting question of where the processing actually takes place, at the seller's end or at the buyers? If the buyer and the seller are in two discrete jurisdictions each of which have different territorially defined laws governing contract formation, this problem could become acute. Needless to say this also has the potential to open a rather large and messy 'can of worms' regarding such matters as taxation.

This issue of jurisdiction has become a matter of considerable concern in the legal community over the past few months. Earlier this year, the Californian based Internet portal site 'Yahoo!' hosted an auction of Nazi memorabilia. By virtue of its presence on the WWW, the portal, and thereby the auction, was accessible across the globe. Under the French judicial system, the promotion or sale of any material which promotes racial hatred is illegal. Pressure from French activists succeeded in a case being brought against Yahoo in a French Court under this law.

A French judge ordered that 'Yahoo!', as it is accessible by French nationals, must comply with French law. This ruling has sent significant 'reverberations' around the international community as it has could cause a serious impediment to global e-commerce, potentially forcing web site owners to ensure compliance with the national laws of every country in which their Web site is accessible. At the time of writing this case is subject to appeal within the French courts and the outcome is unknown.

When is a contract formed?

The general principles of contract formation have been detailed above. However, such principles will, over the course of time, have been the subject of further clarification, by the application of case law. Case law therefore, has a bearing on this issue. I will use two examples from UK law. It is likely that other legislatures will have similar rulings, which may need to be taken into account in considering contract formation.

✦ **The Postal Communication Rule**

This was developed under case law to accommodate problems with contract formation caused by the vagaries of the English postal system in the 19th century. Postal delays meant that communication could no longer be considered instantaneous as with a face-to-face meeting. Under the 'postal rule' a contract is said to have been formed the moment the letter confirming acceptance is posted whether or not the letter actually reaches its destination.

✦ **The Instantaneous Communication Rule**

This holds the conventional view that when communication is instantaneous a contract is formed when the acceptance of an offer is received.

It is remarkable that a law formulated in the 19th century can have a bearing on 21st century e-business, but it does! The law, in the UK holds that if communication takes place over an Intranet i.e. an in-house network, which does not utilise the services of a third party, the instantaneous communication rule applies. If communication takes place using a 'service provider' (Microsoft Hotmail would be a good example) the postal rule applies. It may be possible to construe this rule as having a bearing on customer facing services which are outsourced and where customer transactions are routed through such service providers en route to fulfilment.

For 'contract' read 'transaction'. Now consider this in the context of e-business offerings such as Internet sharedealing or new delivery channels using WAP or Digital TV. There could well be circumstances where the point at which a contract is deemed to have been formed is critical in determining liability in respect of any litigation. Clarification in some of these areas will require case law and one can imagine extended debate among legal briefs over whether an entity that forms part of the routing between a customer and the business be considered a service provider and subject to the Postal Rule.

Under what terms and conditions is the contract formed?

It is usual to clarify the terms and conditions (T&Cs) under which business will be conducted by displaying these on the Website. Typically, the T&Cs include legal disclaimers. If the intention is to target a global market, there are a number of issues to consider in the formulation of such statements. Firstly, the extent to which liability can be lawfully disclaimed will vary from country to country. In the UK and many other countries, this will be constrained by legislation relating to unfair contract terms or legislation relating to defamation (which cannot be disclaimed under UK law). One approach may be to add a statement to say which national legislation applies. However, the legal effectiveness of such a clause may itself need to be tested in other countries. The language barrier itself may pose a legal stumbling block. There is no point in displaying a terms and conditions statement in a language that the customer cannot read. Even if the legal problems can be resolved, regulated products such as those sold by

the financial services industry are subject to stringent regulation in most jurisdictions. The only safe course of action will be to tailor the T&Cs to each country at which the service is targeted which is not an easy thing to do.

Web site disclaimers need to include:

✦ ***A Responsibility statement***

Where there are links on a web page to other sites, users may not differentiate material produced by the Web site owner from material produced by a third party. The statement needs to be clear about what is and what is not third party material. If this is not clear, the Website owner could be held liable for the content of such material.

Note: Note that under English law, if you link to third party material that is defamatory you may be liable for publishing it. It is unlikely that a disclaimer would make any difference.

✦ ***A Liability Statement***

This is intended to disclaim responsibility for anyone taking actions in reliance upon the information. This is a legal grey area as despite the disclaimer it is possible that liability could remain. As a 'rule of thumb' if an individual suffers injury, or damage to property is caused as a result of relying upon the published material there is a greater risk of liability. The situation is more complex with financial organisation as in some countries such as the UK where the advertising of financial products and offering financial advice is regulated under the Financial Services Act, a limit will be placed on the extent to which liability can be disclaimed

✦ ***A Territorial Statement***

A Web site may be viewed by anyone anywhere in the world equipped with a computer, a browser and a connection to the Internet. In some countries products may be illegal, or even if they are legal, advertising them may be regulated in a manner different to the host country. It is therefore important to be clear about the target market.

✦ ***Visibility***

The value of a disclaimer in terms of protecting a company against legal action is directly related to the visibility of the disclaimer to the customer. The 'entry page' approach is considered the safest but may not be popular with the marketing department. The length and clarity of the disclaimer is also a consideration (note: there are issues here relating to 'deep linking' - see the section on hypertext links).

The Territorial Issue and the Regulator

The Financial Services and Markets Act in the UK and similar legislation elsewhere in the world means that investment products are regulated. This means that there are regulatory issues over and above the legal ones relating to the geographical targeting of investment products sold over the Internet.

The FSA in the UK has stated that it will take enforcement action against foreign sites accessible within the UK, which infringe the Act. Clearly it cannot take action against all Web sites accessible from within the UK offering investment products irrespective of the geographical market that they are targeting. It will therefore consider the following:

- is the site located on a server outside the UK
- to what extent is the underlying investment available to UK customers
- to what extent have positive steps been taken to ensure that UK investors do not obtain the investment service as a result of an advertisement placed over the Internet.
- to what extent have positive steps have been taken to limit access to the site
- to what extent are advertisements directed to persons in the UK (visible disclaimers and warnings, pull down boxes for pound sterling, performance plotted against the FTSE, notification of the site to a UK search engine, established bulletin board and newsgroup activity which promotes investments in the UK and advertising the presence of the site in the UK)?

Although this relates to the UK, other regulators may have similar concerns and similar legislation to prevent UK firms targeting their own nationals. This is likely to be the case as the legislation enacted in the UK is based upon the recommendations of the International Organisation of Securities Commissions (IOSCO) Internet task force

DIGITAL SIGNATURES

A digital signature is a means of ensuring the confidentiality, authenticity, message integrity and non-repudiation of data transmitted electronically, e.g. over the Internet. The basic schema associated with any digital signature arrangement uses public key cryptography to ensure confidentiality and non-repudiation, a message digest to ensure integrity and a certification authority to ensure authentication.

The legal standing of Digital Signatures

In 1996 the United Nations Commission on International Trade Law (UNICITRAL) drafted a model law on e-commerce which was adopted as a General Assembly resolution. This noted the increase in international trade transactions conducted by electronic means and drew upon previous resolutions dating back to 1985 on the legal admissibility of computer records.

The model law was intended as a framework for member states to construct their own legislation governing alternatives to paper based methods of forming contracts and storing related contractual information. The model law has a number of provisions.

First, the law recognises the legal validity of electronic data so it would no longer be possible to discount data held electronically as being inadmissible for the purposes of entering into relationships which are legally defined.

Secondly, the law places digital signatures on the same legal footing as hard copy signatures for the purposes of authorising legal relationships subject to a number of conditions concerning the way in which such signatures are designed, encrypted authenticated and validated.

The law recognises the validity of electronic storage as against hard copy storage for the purpose of legal admissibility and makes specific references to the validity of electronic messages in the formation of contracts.

The model law is important because national legislatures, where they have enacted e-commerce enabling legislation, have invariably based their law upon these provisions so there should be some degree of international commonality in the law applying to this area.

In the UK the provisions have been enshrined in the Electronic Commerce Act which gained Royal assent in July 2000. It provides for:

- an approvals scheme for business and other organisations providing cryptography support services such as electronic signature services and confidentiality services
- the legal recognition of electronic signatures and the process under which they are verified generated or communicated and
- a basis for the removal of obstacles in other legislation to the use of electronic communication and storage of paper.

The passing of e-commerce enabling laws is not confined to the UK, for example the Hong Kong Electronic Transactions Ordinance was enacted on 7th April 2000. In the United States, the National Conference on Uniform State Laws (NCUSL) is working towards a Uniform Electronic Transactions Act (UETA) to harmonise local state laws on e-commerce and in Japan a bill covering the legal recognition of digital signatures was recently submitted to the Japanese Parliament (Diet) and is likely to pass into law sometime in 2001.

The term 'enabling laws' is used advisedly. It is important to recognise that e-commerce legislation, where it has been enacted on the basis of the UNICITRAL model law, removes the legal impediments to legal recognition of digital signatures and the legal admissibility of electronic data. In short it provides the legal foundations upon which to 'build the house'. What it does not do is replace the raft of secondary legislation which regulates UK industry. This can only be modified by the relevant legislature or regulatory bodies. Some examples from UK secondary legislation would include the following:

- the 1987 Banking Act in the UK which provides the general framework for the conduct of Banking business for UK deposit takers and
- the UK Consumer Credit Act which requires that certain types of credit agreements must be physically signed.

In addition to this there are other types of secondary legislation which have an impact upon contracts and need to be taken into account in considering Web site terms and conditions. A good example would be the Unfair Terms and Consumer Contract Regulations, which were implemented in the UK in 1995 following EC legislation. These regulations control the formation of contracts between 'unequal parties' and allow a court to strike out contractual clauses which it considers to be 'unfair'. There is an extensive list of clauses that would be considered by the courts unfair detailed in schedule 3 of the Act. These include restrictions on liability, general opt-out clauses, restrictions on legal remedies, 'hidden clauses' and so on.

It is significant that in looking at the statistics provided by the Office of Fair Trading that the financial services industry together with double glazing companies and mobile telephone operators have been the subject of most of the court actions to date under these regulations.

Unfair Contract legislation is now finding its way into the laws of countries such as Thailand which passed an Unfair Contract Terms Act in 1998.

Additional EU legislation (directive 97/7/EC) is being introduced over a transitional period in the UK to regulate distance selling. This legislation is applicable to any organisation using the Internet to sell goods and services to EU nationals and enforces four basic rights for consumers:

- a requirement for supplier to provide prior information to consumer
- a requirement for written confirmation of this information to be provided by the supplier
- a cooling-off period of 7 working days for a consumer to cancel the contract
- a requirement for delivery of goods or services within 30 days, unless otherwise agreed
- and restrictions on use of unsolicited marketing communications.

The financial services industry was explicitly excluded from this directive but there is a proposal to introduce a specific directive to regulate the distance selling of financial services. At the time of writing this is still under discussion.

Legislation also empowers regulators to construct a regulatory framework for the conduct of financial services business. Compliance with this framework is additional to legislative requirements, (e.g. compensation rules for product mis-selling, operational risk management, the conduct of outsourcing etc). There is an attempt at the global harmonisation of regulatory rules for securities through the International Organisation of Securities Commissions.

COPYRIGHT AND TRADEMARKS

Copyright

Copyright generally arises automatically, in that it doesn't have to be registered. The contents of a web site will benefit from automatic copyright protection in the same manner as literary, artistic and sound recordings. It also applies to such issues as Web Site design.

This could be a potential issue for a company using a Web site design agency in that copyright will remain with the agency unless there is a specific clause within the contractual relationship that assigns copyright to the company.

It is also advisable to ensure that the agency confirms in writing that any design produced does not infringe the copyright of any other agency or client.

Continued on page 25

NETWATCH

By Annabel Lane, Nestle UK Ltd

The theme of e-commerce is still keeping many of us busy, and as you may well have noticed, this edition of Datawatch picks up on the legal aspects of electronic transactions. So it seemed worthwhile to continue with the e-commerce theme, as well as looking at a few other sites that may be of interest.

http://www.ecommercetimes.com/

This site's name is suggestive of a newspaper, and that essentially is what it provides - a plethora of headlines associated with the area of e-commerce. If you are looking for anything in particular, there is a search engine which you can use to bring up articles on the site as whole. The site claims to be updated every 5 minutes, twenty four hours a day, so you should always be able to get the latest stories here - there are even sections at the bottom of the front page for stories that have broken in the last 15 minutes. The top banner offers several more options, including special reports with more in depth stories and an area dedicated to CRM. (Customer Relationship Management), a very hot topic at the moment. This area contains more stories dedicated to this particular subject, such as what the main industry players are doing. All in all this is a pretty comprehensive site with links to other areas in e-commerce and even a space dedicated to the top internet stock options….not that any of us would be interested in that sort of thing…..

http://www.tgt-associates.com/

This is an offering from a company dealing with e-commerce and IS security aspects. I quite liked the benchmarking survey that they have on the site- answer 17 questions ranging from the main business of your company to the hacking, viruses and phreaking that you have experienced, and they will email you a report telling you how you rate compared to other respondents. If any one dares to actually do this, please let me know! I am sure they don't name names…! Once again there is a news page which offers you headlines broken down by category - security, Linux, e-commerce, internet, etc. Naturally they are promoting their own seminars and risk management tool.

http://web.mit.edu/security/www/gassp1.html

Gassp sounded to me like last gasp, but it in fact refers to Generally Accepted System Security Principles of the International Information Security Foundation. The idea is that this body is supported by both industry and governments to develop and promote proper security principles throughout the world. Committee Members hail from the US, the UK, Canada, Mexico, Japan, Sweden, etc. You can download the document of security principles in MSWord or zipped format. Essentially the principles to be used are the OECD ones, but the document goes into a lot of detail, starting at a high level, defining the basic principles it considers essential, such as accountability, awareness and ethics. It then explains these and goes into more detail as to what it expects management to do to uphold these principles and gives some rather interesting examples of what can happen as cautionary tales. Additional material after the main body of the text talks about risks to computer usage which is also of interest.

http://www.ecrc.ctc.com/about.htm

This is the web site of the US Electronic Commerce Resource

Centre which assists industrial and government organisations in e-commerce matters. The front page, after explaining what the ECRC is and aims to do, has a brief resume of what electronic is and what its benefits are, especially to government entities. Its practical use is probably limited to those of us in the UK, but it is interesting to see what initiatives are underway and how e-commerce is being used. I have heard there are quite a few companies out there where management are huddled at the boardroom table, agreeing that they should be "into" electronic commerce - but how and what? There's a wealth of information in this site, though it's not immediately apparent - try looking at the online resources and some of the reports they offer. At the top of the list is JECPO, the Joint Electronic Commerce Programme Office, whose website has links to many different pieces of information and publications. For example, under publications you can download the EC handbook which has an extremely comprehensive range, from what e-commerce is through the technicalities regarding VANs (not the sort that get driven!) to who is involved in what initiatives.

http://www.sfisaca.org/

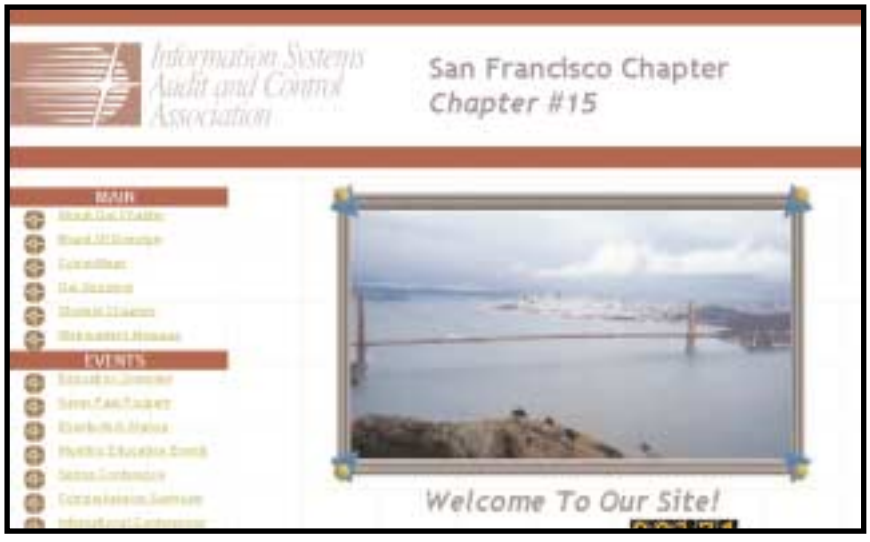
You of course are all familiar with the web sites of the UK Chapters, but there are other Chapters of ISACA round the worlds who also have sites. This one, belonging to the San Francisco Chapter, was brought to my attention recently. It has a very impressive front page with a picture of the Golden Gate Bridge, and there are plenty of other aspects of the site as listed in the index on the right hand side, which may be of interest. As you'd expect there is a resource list of sites on the subject of Audit and control, firewalls, IS Security, etc., and you can download their quarterly newsletter, which is award winning like this one - and elsewhere in this edition, you can read about our plans for the web site and the addition of Datawatch content to it.

http://Wap.com

There's been a lot of comment recently about the failure of WAP to break into the market in a big way, and quite a few commentators have been dismissing it as something that won't really take off as planned. Whether you think this is the case or that the technology still has to mature a bit further to offer the benefits that have been promoted to us all. This site, which as you may guess from the title is all about WAP is quite upbeat. It describes itself as your guide to the wireless internet and certainly seems packed with information. There are reviews of WAP sites, reviews of WAP phones to guide you as to which one is best for you, and they promise to review all the new phones as they come onto the market. There is also a large resource list, which details WAP sites by category - there is also a more normal web site alternative. You can also try the Wapaliser. This is an emulator to give you the idea of what it will really be like using a WAP phone - what those WAP enabled sites will really look like using a Nokia 7110. Now that's interesting to see.

http://www.itsecurity.com/reference/ic2000.htm

And finally for the really paranoid among us….is Big Brother really watching us all? Or if not, how easily could he be?? This site is all about interception of communications - something that's been a hot topic recently with the debates surrounding the RIP bill. This is a great one for the conspiracy theorists as it lists government co-operation initiatives in the area of comint (communications intelligence) and all the various ways that data transmission can be intercepted.



Programmes have names like "Shamrock" and systems like "Echelon", just to add an air of additional mystery. But seriously, this has a point. If you look at the different ways your communications can be intercepted and who is behind some of this, it may make you think just how private your daily conversations really are…..

To end, as usual, on a slightly lighter note, here is a joke I heard recently on that old theme of the usefulness or otherwise of consultancy. It made me smile and also think about the high tech methods the consultant uses to work out something that was already known….are any of use ever guilty of such a thing??

A yuppie in an SUV is driving through the highlands of Scotland. He comes across a shepherd with a flock of sheep. He drives straight up to the shepherd and tells the shepherd that he will guess the exact number of sheep in his flock in exchange for a sheep of his choice. The shepherd looks bemused but he agrees to the challenge.

The guy climbs into his SUV, pulls out his laptop, connects to a satellite which beams down an infrared image of the hill. He then feeds it into an image processor which spits out the exact number of sheep on that hill. He jumps out of his vehicle and tells the shepherd: "Dear sir, you have exactly 1280 sheep in your flock."

The shepherd is impressed and agrees to keep his end of the deal. So the guy picks a sheep of his choice and as he is putting the sheep in his car, the shepherd asks: "Sir, if I were to guess what you do for a living, can I have my sheep back?" In all fairness the young man agrees.

The shepherd says, "You are a Consultant." So the young man exclaims, "You are absolutely right! But how could you tell?"

The shepherd replies," First, you offered me your services without me asking for it. Then you told me something that I already knew. And finally you have no idea what you're doing-- because that's my sheepdog you're putting in your car."

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
http://www.infosyssec.org/infosyssec/index.html
http://web.mit.edu/security/www/gassp1.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
www.sap.com/mysap/

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
http://e-commerce.internet.com
http://www.ecrc.ctc.com/about.htm

The Electronic Original Initiative

A major new audit/ compliance opportunity for ISACA and its members

THE NEED

Most companies today operate as e-businesses whether they realise it or not.

What they probably do not realise is their need to meet legal obligations for: -

1 Evidence at Court
2 Audit
3 Director's Duty of Care
   - in retention of records of their e- business operations.

The Electronic Original Initiative has developed 5 International Codes of Good Practice that set technical and operational "standards" for e-business operations. The Codes cover:

- ✦ E-documents, e-mail, fax and e-commerce transactions
- ✦ The use of digital signature technology
- ✦ Certification Authorities
- ✦ "Electronic original" storage and retention

THE START

For hundreds of years paper has been an acceptable way for businesses and other organisations to store their documents. A paper storage process is required for:

- ✦ Audit
- ✦ Reference
- ✦ In case of legal challenge
- ✦ To comply with legal and audit requirements e.g. company law

The legal position on company records in electronic form is not clear-cut. In legal disputes electronic evidence is sometimes accepted and sometimes not. In 1994, 150 representatives from the U.K. Government, the legal profession and industry addressed this unhappy situation in the UK. It was determined that three parallel activities were required:

1 Production of Technical Codes of Good Practice for the storage of Documents in Electronic Form
2 Changes in the law over time to remove outstanding obstacles
3 Development on an international level

Production of a UK Technical Code of Practice

Following two years of work co-ordinated by ourselves and involving some 130 organisations, the British Standards Institution (BSI) issued a technical Code of Good Practice in February 1996.

The purpose of the initial Code was to set a standard of system and process controls to give confidence that records had been stored and retained according to best practice. Similar codes exist and have been successful for microfilm and microfiche. Companies and organisations need to audit their systems and processes annually for compliance.

In practice record retention under this Code is subject to far more controls than those applied to paper and therefore arguably the electronic record should carry more weight for legal purposes than its paper equivalent. BSI launched the Code in February 1996. The launch meeting was oversubscribed and some 1200 companies attended subsequent road show meetings around the UK. Currently BSI is organising regular quarterly workshops at which some 40 organisations are being trained to self-audit their companies' operations. Private companies also provide independent audit services.

Role of The Electronic Original Initiative

The Electronic Original Initiative management, which played a major role in the development of the original Code, decided to take this activity to the next logical stage by instigating six major initiatives:

- ✦ Extending the range of the Code
- ✦ Expanding its application internationally
- ✦ Setting up an International Review Panel
- ✦ Obtaining the support of International Publishers
- ✦ Initiating a process of legal change
- ✦ Co-ordinating a broad based promotional campaign.

Extending the Range of the Codes

A new code in 5 parts has now been issued. The 5 parts cover:

1 Electronic storage
2 Electronic transmission
3 Digital ID, Signature, and ownership
4 Verification of (3)
5 Trusted Remote Archiving

The Code is designed for international acceptance; in other words for use with systems and processes that will be accepted world-wide. It is also designed to inter-link in a dependence hierarchy starting with the first part (electronic storage)

CISA Exam 2000

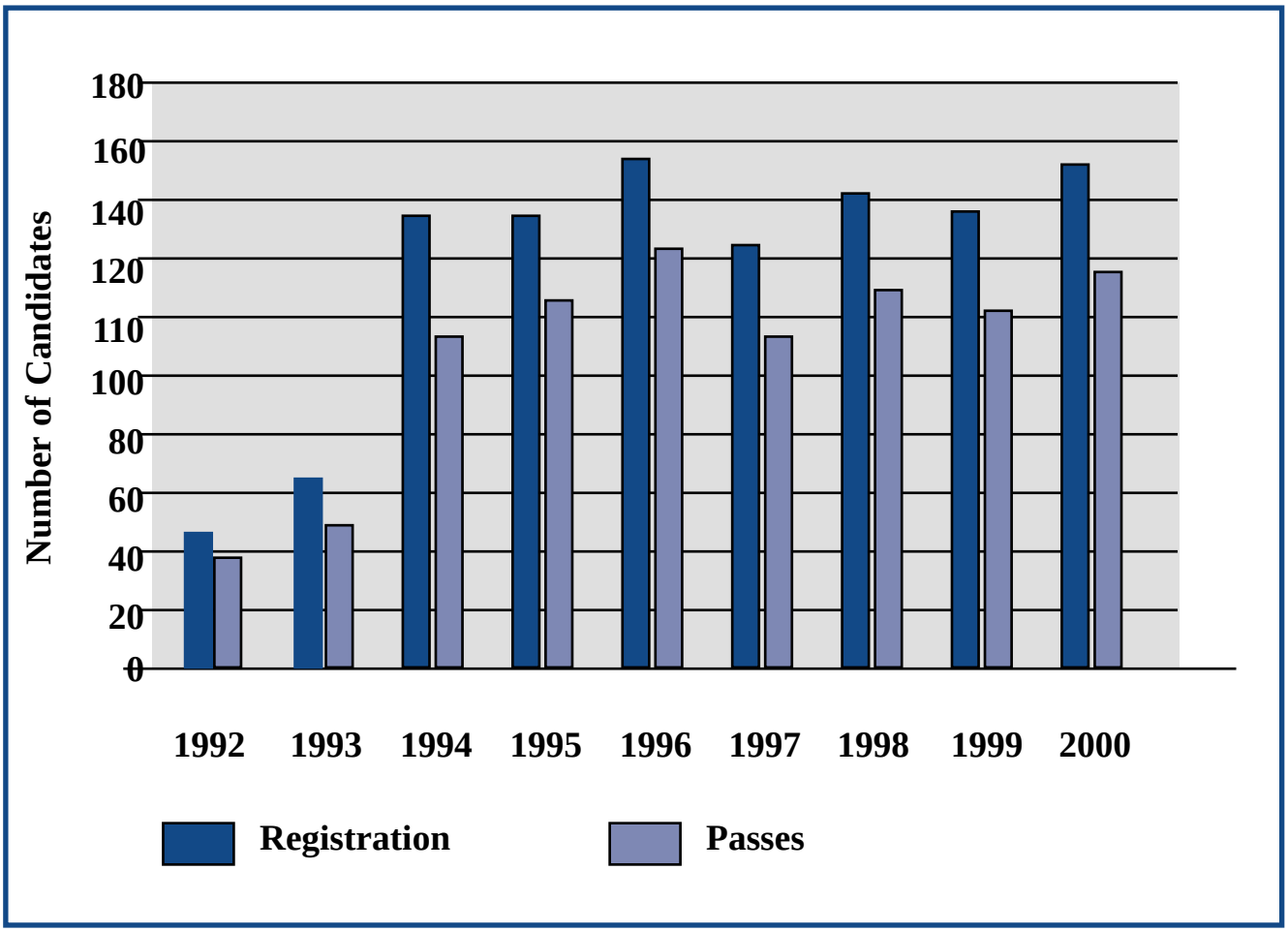
By David Spaven, CISA

Congratulations to all successful candidates! Yet again the candidates sitting their CISA examinations at the London centre have shown their outstanding abilities with a 77.1% pass rate compared to a declining global pass rate of 52% (54% in 1999).

This year saw another record with 6,458 candidates registering for the examination globally, and 153 sitting the exam in London.

As the graph indicates the success rate over the last 9 years has been consistently in the high seventies which is an outstanding achievement.

The graph also indicates the continuing high level of interest of people following our profession in obtaining the CISA designation. There was a peak in 1996 where there was a surge of candidates from the financial sector. Although official statistics are not yet been released, initial analysis indicates that this years candidates were again drawn fairly evenly from across all industry sectors. Within the London area, the majority of candidates were from the big five practices, and from the financial services sector, but commerce and industry was also well represented. This indicates a continuing trend in awareness of the benefits of using IT audit and security specialists in all sectors.



Congratulations to the following 125 London Chapter candidates who successfully sat the 2000 CISA exams in London and other regional centres:

Mr. Christopher Azzopardi, CPA
Mr. Mark E. Bailey
Miss Denise Barnett
Mr. Kevin Charles Barron
Mr. James E. Barton
Mr. James L. Bate, MAAT,CAT
Mr. Graham W. Beckram
Miss Alexandra V. Beere
Mrs. Seema Bhandal
Mr. Vipan Bij, MBCS
Mr. Daljit S. Bilkhu
Mr. Michael Adil Boneh
Mr. Colin Ralph Bootes
Mr. Avinash Jaydev Brahmbhatt (1)
Ms. Victoria Ellen Brinkley
Mr. Peter J. Brophy
Mr. Christopher John Browm
Miss Claire T. Carleton
Ms. Jaquelyn Castle
Mr. David Jesus Castro
Miss Helen Olivia Clay
Mr. Timothy Ashley Clough
Mr. Michael Collins (3 =)
Mr. Jeremy Robert Darnell
Mr. Sunil Nanikram Daryanani
Mrs. Dilani Dassenaike
Mr. Edward Alfred Jonathan Dav
Mr. Simon Forsyth Davidson
Mr. Steven Day
Mr. Jason Christopher Day
Miss Gillian Carol Dickie
Mr. John Alexander Dobbs
Mr. James Draper
Mrs. Claire W. Edwards
Ms. Rosaleen Enemuwe
Mr. Vito Fava
Miss. Carol Janet Franks
Mr. Ian Gilbert
Miss Eana Vera Gillies
Mr. Christopher John Gray
Mr. Mark William Hallam (3 =)
Mr. Peter R. Hanney
Mr. Stephen John Heath
Mr. Marcus L. Hebbes
Mrs. Maninder Kaur Hoyle
Mr. Niall Hughes
Mr. Christopher M. Hussey
Mr. Robert I'Anson
Mr. Richard Jenkins
Mr. Gareth Owen Jenkins
Mrs. Laura Bridget Joint
Mr. Mario Christy Joseph
Mr. Philip C. Joyce
Mr. Jonathan Robert Keefe
Ms. Isabel M. Kershaw
Mr. Amandeep Singh Khosa
Mr. Joseph C.L. Kiddell
Mr. Paul A. Kiff
Mr. Steven Matthew King
Mr. Eric Ivan Long
Mr. Colin Neil MacKenzie
Mr. Donald MacQueen
Mr. Manyu Malhotra
Mr. Adan Shakoor Malik
Mr. Lawrence Philip Mangelshot
Mr. Paul Williams Manning
Mr. Richard Charles Mansell
Mr. Paul Brian Matthews
Mr. Garry John McCubbin
Mr. Kieran Thomas McDonagh
Mr. Michael Charles McGuffie
Mr. Andrej Miller
Mr. Marc Anthony Monasingh
Mr. Andrew David Morris
Mr. Justin Joseph Mycroft
Mr. Michael Jason Neutens
Mr. Daryl Peter Thomas Norman
Mr. James Joseph Norminton
Mr. Manoj Odedra
Mr. Peter James Osborne
Mr. Ross Palmer
Mr. Matthew Keith Phillips
Miss Vanessa Pillay
Miss Preeti Chandana Pochun
Mr. Netan Popat (3 =)
Mr. Gideon P. Pretorius
Miss Yasmeen Rahman
Mr. Jason John Reading
Mrs. Judith Redfearn
Mr. James Thomas Rigby
Mr. Antonio Manuel Rodrigues
Mr. Michael John Samways
Mrs. Genevieve Danielle Schust
Mr. Nicholas J.R. Seaver
Mr. Fagun Shah (2)
Mr. Geoffrey A. Shaw
Mr. Daniel Ogola Siage
Ms. Lynette K. Siemers
Mr. Albert Kipkemoi Sigei
Mr. Robert Michael Smith
Mrs. Caroline Anne Squire
Mr. John S. Stewart
Mr. Douglas Stewart
Mr. John Anthony Sutherland
Kishor P. Tanna
Mr. Aaron J. Thomas
Mr. Derek Anthony Underwood
Mr. Gagan Verma
Mr. Jason Edward James Viola
Mr. Martin John Vipond
Mr. Martin John Wale
Mr. Andrew Peter Ward
Mr. Nigel John Watts
Mr. Aaron Keith Weller
Mr. Mark Ivan Werner
Mr. Mark Stephen Wilde
Mr. Nigel Yazdabadi

Our special congratulations to the following London UK Chapter members who achieved top scores in this year's examination:

1st - Avinash Brahmbhatt
2nd - Fagun Shah
Joint 3rd - Michael Collins, Mark Hallam and Netan Popat

such that transmission requires code compliant storage and a transmitted ID requires both code compliant storage and transmission (see Fig 1 below).

Business Benefits

The Codes of Good Practice provide:-

1 Protection from the vulnerability of effecting e-business operations without due care for business obligations
2 High levels of bottom line cost savings.

How many companies have e-mail retention policies that protect their Directors' Duty of Care obligations to record key company documents?

What arrangements have you made for e- commerce and e-invoicing operations?

On the subject of cost savings, research carried out by Xerox, Pitney Bowes and ourselves puts some parameters on the costs of paper based document systems and the benefits of moving to secure "electronic original" operations:-

- The life cycle cost of a document is $10
- A search of a paper archive for a document can cost $75
- Most companies now use computers and in many cases the original of a document is in electronic form. It has been estimated that 70% of company documents are generated on PC's.
- The average electronic transmitted document volumes and transmission costs of Fortune 500 companies are:

  - 250 million documents sent and 250 million received per company per annum
  - Document transmission expenditure (predominantly faxing) is running at some $17m per annum per company; this represents 40% of the telecommunications bill.

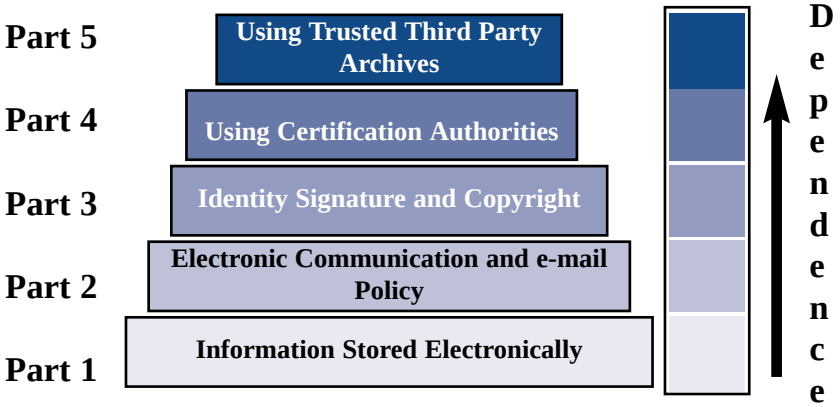


Fig 1. Relationship between the 5 codes

- The costs of running a paper only solution is not sustainable when cheaper and more efficient methods exist
- This cost is increasing at c20% per annum.
- Fax and e-mail will shortly overtake real time telephony as the dominant communications medium between companies. Growth is 25% per annum
- Cost savings of 25% on the $10 document cycle cost are achievable from "electronic original " based trading. All companies would gain pro rata. This is a saving of $2.50 for each "electronic original" stored document
- Paper based document systems have only been retained because no clear route for companies has existed to transfer to "electronic original" based trading - until now

Opportunities for ISACA and its Members:

These Codes offer the ISACA a number of business opportunities to play a major role in the development of standards and audit of e-business operations. Briefly, these are:-

1 as a publisher/distributor of the Codes
2 in providing training courses to its membership in audits for compliance with the Codes
3 to join the Electronic Original Initiative Advisory Board
4 to develop the Codes with BSI and ourselves to cover e-business financial audit processes.
5 to develop processes for e-commerce fraud prevention based on the above.

For individual ISACA Members the Codes of Practice offer a major new audit/compliance service opportunity.

Where financial audits were the central audit service for all organisations in the 20th Century. In this century e-business "legal"operations audits will become the new focus of attention. In this space the EOI Codes of Practice will be central.

The EOI is in dialogue with ISACA. If you are interested in keeping in touch with this development, please contact:-

Malcolm Smith
Electronic Original Initiative Ltd.
3 Wintergreen Lane
Wallingford
Oxfordshire
OX10 9EN
United Kingdom
Phone: 01491 837456
Fax: 1491 825720
E-mail: m.smith@g5group.com
www.the-eoi.org

Telephony Security - Denial of Service Attacks

By Duncan McKerracher

In Issue 42 of Datawatch, we outlined the four main issues of telephony security - Toll Fraud, Denial of Service, Corporate Embarrassment and Phone Tapping. Previous editions have featured Toll Fraud and Corporate Embarrassment. The next edition will describe Phone Tapping. This article describes an issue that has seen a worrying increase in incidence over the last year, that of Denial of Service.

Denial of Service is where the hacker affects the performance of a telephone network with the aim of reducing the efficiency of an organisation's routine business. In certain cases, the hacker can completely destroy the telephone service leaving the organisation unable to perform even the most basic functions. In extreme cases, this has even led to the closure of companies whose business depends on the full time availability of their telephone system.

Denial of Service attacks are generally carried out by Commercial Hackers or Disgruntled Employees. Commercial Hackers are employed by rival organisations with a view to gaining a commercial advantage by disrupting their competitor's business. Disgruntled Employees are privy to classified information about their organisation's system. The Disgruntled Employee also includes ex-employees or sub-contractors who have a grudge against their organisation. They represent a serious risk in that they have extensive knowledge of the telephone system they and often know how to gain easy access to it.

There are three main ways in which a Denial of Service attack can be carried out. These are as follows:

Unauthorised reconfiguration of telecoms systems

Unauthorised access to the maintenance terminal of the PABX can allow the hacker to redirect inbound calls to inappropriate destinations. This often allows the hacker to make fraudulent calls to effect Toll Fraud. However it can also allow the hacker reconfigure the PABX to stop working altogether. Most PABXs have a command that is used to shut it down completely. If this is achieved then an organisation will have no telephony services whatsoever.

Physical damage to telecoms systems and services

One of the crudest forms of telephone hacking is where the hacker causes physically damage to an organisation's telecoms system resulting in their telephony services becoming inoperable. This can be

Example No. 1

Public Telephone Operator - South East England

The merger of two telecommunications companies resulted in the redundancy of a number of technical support staff. One of the staff who lost his job decided to exact his revenge by disrupting the newly-formed company's internal telephone network. His expertise allowed him to set up a call between two offices that generated another call, then another, then another in a series known as "tromboning". This had the effect of busying the network then overloading the company's PABXs such that they ceased working altogether.

It took over 5 hours to rectify this fault in which time there was no means of internal or external communication for the new company. It was impossible to put an exact figure on the cost of this disgruntled employee's action, but an estimate of £25,000 in lost productivity is not far off the mark. This takes no account of obvious frustration and embarrassment.

Fortunately the employee decided to restrict his action to the internal corporate telephone network and not their Public Telephone Network used to serve its customers. If this had been the case the cost would have run in to many millions of pounds.

carried out by an outsider where there is poor physical security, or by a disgruntled employee with access rights to the equipment room. Although this remains a relatively rare form of hacking, its effect can be catastrophic given that the damage is usually permanent with a relatively long time for recovery.

It should be noted that this form of hacking also extends to an organisation's network service provider (e.g. BT, cable companies). Therefore careful consideration must be given to the physical security and diversity of its incoming services.

Overloading of Telecoms Network

In the past, this form of hacking has been carried out by disgruntled employees who have a detailed knowledge of their organisation's telephone system. This involves setting up a multitude of telephone calls on an organisation's telephone network with the effect of overloading the PABX and its trunks such that staff cannot make internal or external calls. Additionally, inbound callers (i e. customers) cannot access staff within that organisation.

This has caused particular problems within organisations that rely upon their call centres for daily business. In extreme cases the telephone network been totally disabled owing to such action.

The examples are real life Denial of Service attacks that have taken place over the past two years. They show that Denial of Service can be a real risk to your organisation's. Many organisations remain unprotected against this risk. By implementing simple procedures such as updating network configuration, improving physical security and adopting new management procedures, it is possible to minimise the risk of Denial of Service at a relatively low cost.

Duncan McKerracher BEng is an independant Telecoms Consultant specialising in Fraud and Security issues. He is a member of the Telecommuncation Manager Association. He worked in the Ministry of Defence for over 10 years and has since helped more than 50 large companies combat telecommunications fraud.

Example No.2

Financial Organisation - Midlands

A financial services company relied upon the availability of its call centre to support its business. A hacker managed to dial into the maintenance terminal of the company's PABX via an unprotected modem. The hacker used a number of commands to completely disable the PABX. This had the immediate effect of preventing customers from dialling into the call centre. It was over two hours before the fault was identified and rectified. The estimated cost to the company of lost business was £100,000.

Example No. 3

Large Hotel - London

A "telephone engineer" arrived at a hotel and asked the receptionist for the keys to the PABX room to allow him to rectify a fault. The receptionist stated that there were no problems with the telephone system and had some reservations, but duly handed over the key to the engineer. An hour or so later he left the premises. Later that day he returned again asking for the keys to allow him to rectify a further fault. This time the receptionist had no hesitation because she was aware of a number of guests who were experiencing a loss of service. After another hour he left the hotel.

By this time there were no service to any of the guestrooms. The hotel manager was called, and on visiting the PABX Room, he discovered that the "telephone engineer" had removed all hardware leaving an empty PABX cabinet. The hotel was left with a much-reduced service for over two days and a bill for £30,000 to replace the stolen hardware.

10 YEARS AGO

CISA EXAMINATION

The following item appeared in the November 9th Issue in 1990, making an interesting comparison with David Spaven's current article on pages 14 and 15:

"The examination was held on Saturday 16 June at over 100 centres around the world including London and Manchester. Of those sitting the examination in London 35 were successful and all seven of the candidates from Manchester passed the examination. Congratulations to each and everyone of them.

In total around the world there were 2,258 candidates and 1,482 were successful this year. Within Europe. it is interesting to note, the number of EDPAA members and the number of successful students who passed the 1990 examination:

Country	EDPAA Membership	No of Passers
Spain	127	16
France	55	25
Germany	29	1
Denmark	154	5
Holland	109	10

Website Update

By Allan Boardman

If you have recently visited the ISACA London Chapter website, you may have noticed a few changes.

This is an overview of some of the main changes and some other initiatives in the pipeline. Recently added or updated:

- The events programme for 2000/2001 has been updated, around the theme "IT Governance in the e-economy.
- Booking for the monthly events is now available online. Completion of the online booking form will generate an email to Nancy and your information is not held online.
- Back copies of feature articles from Datawatch are now available to members under the Publications tab. Articles from back copies will be made available as new editions are published.
- There is now an on line discussion board for use by visitors to the site to engage in debate, sharing of views or posting questions or comments. A reminder, avoid using personal names, use initials or online pseudonyms instead.
- Updated Internet Resources - always useful in your search for information if google does not excite you or jeeves leads you down the lycos.
- Details of the successful candidates (who wrote in London) in the CISA 2000 examinations has been included.

Coming soon or under discussion:

- An online survey feature is currently under development. The first survey will be used to solicit members' views on the preferred time for the Thursday meetings.
- Members restricted area. The main ISACA site already has an area restricted to members (www.isaca.org/@member). This part of the site contains three primary components; access to the IS Control Journal, access to Global Communiqué, and web based change of address. There have been some discussions on whether certain parts of the London site should be restricted to members, but this has not been finalised. We wish to avoid the need for registration or keeping members' details online. Perhaps the online survey can be used to gauge members' opinions on this.
- The structure and format of the site is planned to change so watch this space, the website space that is!

Finally, see below for some website statistics that shows that there has been a steady increase in traffic over the last six months.

INVITATION TO TENDER

The London Chapter of ISACA invites CISA qualified members to tender for presenting the 2001 CISA review course.

This is the sixth year that the London Chapter has offered the CISA review course for candidates sitting the CISA examination. The course has rapidly become a valuable service to our members and is usually run over nine two - hour evening sessions during April and May.

For a copy of the ITT or to discuss the invitation further please contact:
Michael Christodoulides
CISA Review Co-ordinator 0171 311 5620
Nancy Watt
Chapter Administrator 01487 815 705

The Security Column

By John Hunter

I was pleased to hear on the radio today on the news that using credit cards on the internet is apparently unsafe. The article reported that retailers are losing enormous amounts of money from credit card fraud through internet trading, something that tends to get overlooked in the race to e-trade.

Join the fraud prevention SIG and find out more how to combat this problem.

Summer - a period of relaxing and time to spend on your favourite leisure pursuit. At least that seems to have been true for the hacking community as it has been a pretty active period with an incredible number of big names suffering public denial of service humiliation over the last few months.

There have been a number of recent reports about increased targeting of the LINUX platform. Superseding previous distributed denial-of-service tools, such as Tribal Flood Network and Trin00, (used earlier in attacks on Web sites owned by eBay Inc., ETrade Group Inc., CNN and Yahoo Inc), a new tool, 'Trinity III' has appeared.

The way Trinity works is interesting and an understanding gives a useful lesson to those responsible for security. Trinity is first covertly installed on a server. The server is then remotely controlled, usually together with other similarly compromised computers, to launch a packet flood against targeted machines. The Trinity tool is sophisticated because it lets attackers control the hacked machines through IRC channels or America Online Inc.'s ICQ chat service.

There have been reports of up to 400 hosts running the Trinity agent. In one Internet Relay Chat (IRC) channel on the Undernet network, there are 50 compromised hosts with Trinity running, with new hosts appearing every day. It is not known how many different versions of Trinity are in the wild.

Trinity attacks illustrate a larger concern about LINUX which being open-source is available to everyone, but can end up in the hands of inexperienced staff who are unqualified to install and run them. One answer used in some installations is to scan your network to detect new Linux operating system installations and to determine which ports are used on the machine for new services that could present a risk.
Scan all systems for port 33270 connections. If any connections are found, telnet to that port and type "!@#". A system has been compromised if there is a root shell present after a successful connection to port 33270.

Systems connecting to IRC channels without reason should be looked at immediately. Since the Trinity v3 agent does not listen on any ports, it may be difficult to detect unless you are watching for suspicious IRC traffic. If a machine that has a Trinity agent installed is found, it may have been completely compromised. The operating system might have to be completely reinstalled along with any available security patches. In general public chat systems can pose a security risk. It's fairly anonymous for an attacker to go onto an IRC chat system and launch attacks.

Trinity is capable of setting eight types of flood attacks that can be sent for any length of time. The rogue code simply listens to port 33270 for connections and then attempts to get root shell access when someone logs on.

It really is important to keep up-to-date with the vulnerabilities to keep your site safe.

Happy guarding!

Answers to Linkages on page 4.

1. Off
2. Chip
3. Root
4. Money
5. Cart
6. Electric
7. Elephant
8. Early
9. Mark

The initial letters of these answers form the word "E-Commerce"

Recruitment

By Adrian Simpson BSc ACA FIIA

There are not many things that have become so deeply unfashionable, quite so quickly, as Y2K.

Whilst who mugged who, may be a matter of debate, the phenomenon certainly cast a long shadow over the computer audit recruitment market. As might be expected, given that the economy remains on an even keel, nine months later a semblance of normality is returning.

So, how are things in this normalised world of computer audit recruitment? Well, there are three broad areas of experience that are in demand.

First, whilst the new systems development dams have hardly burst open, the freezes that were widely in place during the run up to Y2K have now largely thawed. Computer auditors with project management experience, a perennial requirement rudely interrupted by Y2K, are now back in demand

Secondly, e-commerce is becoming a huge growth area. Many companies who are recruiting computer auditors recognise that e-commerce is so new that there are bound to be a shortage of people with specific experience of auditing it. In hope rather than expectation, it is currently the most common requirement that employers request. Related skills gained in networks, firewalls and web architecture certainly help.

Thirdly, experience of risk management. This can be a difficult requirement to nail down. However, computer auditors cannot be oblivious to the risk management and control issues raised by Turnbull. As the deadline for reporting compliance looms, experience or an appreciation of risk management has become increasingly common in computer audit job descriptions. Computer auditors who can demonstrate that they can deliver more than purely technical recommendations and can add to the risk management process are in demand.

After the lows of last year, the market for computer audit skills, whilst improving, is also changing. The usual requirements of youth, qualifications (both academic and professional) technical experience and evidence of the ability to adapt to new environments, remain. However, it is important to remember, and this is applicable to general and computer auditors, that internal auditing is changing and so are the expectations of the companies who employ it. Making up the numbers, being the best of an inappropriate bunch, is no longer the game. The vast majority of internal audit departments will carry a computer audit vacancy or use contract staff until they find someone who they genuinely believe is going to make an appropriate contribution.

"...general auditors are acquiring more I.T. skills than ever before."

Whilst unemployment amongst computer auditors still exists, it is more voluntary than the forced type that was evident this time last year. For any established computer auditor who is determined to work there are opportunities in the contract market and if they are prepared to relocate most likely in the permanent market too. The major restriction is not the total aggregate demand for computer auditors in relation to the supply of expertise. It is more that demand tends to be concentrated in London and the South East whereas the supply of expertise is more evenly distributed around the country.

The amount of rationalisation throughout both the private and public sectors has resulted in a lower number of internal audit departments employing a smaller number of computer auditors. This has resulted in significantly reduced numbers of opportunities in many parts of the country. Whereas a few years ago you may have lived within commuting distance of ten internal audit departments that employed computer auditors, it may now only be five. This is a problem that affects general auditors but it is compounded in computer auditing by the greater propensity to contract out.

Paradoxically, just because computer auditors may find it more difficult to secure new positions, does not necessarily mean that companies are finding it any easier to recruit. Experienced computer auditors are generally recruited from other local departments. But what if they no longer exist?

It is interesting, as I.T. continues to become all pervasive, that general auditors are acquiring more I.T. skills than ever before. In fact, when the issue is raised, I am no longer surprised just how much many general auditors know about computer auditing - it goes well beyond the basics. It has become common for general auditors to complete CISA or QiCA examinations.

Now I do not believe the old refrain, that all internal auditors will become computer auditors, is coming to pass. However, the belief that computer auditing is purely a technical discipline should not be the prerogative of a computer auditor. At least not one wanting to ensure that their services will continue to be gainfully in demand.

Central News

By Michael Hughes, President, Central UK Chapter

Congratulations to the members of the Central Chapter who recently passed the CISA exam.

Congratulations in particular go to the top three scorers for the Birmingham test centre: Richard Johnson from Chelsea Building Society and in joint second place: Ian Likeman, also form the Chelsea Building Society and Martin Wale from KPMG. I am pleased to say that just over half of the membership now have the CISA designation, for the rest of you there is plenty of time to register for the 2001 exam!!

Whilst I am giving out congratulations, then well done to Chris Murphy of the West Bromwich Building Society, who was the lucky winner of the prize draw from all those of you who returned their completed membership survey.

Whilst I am on the subject of the membership survey, the main results concerning the format of evening meetings were as follows:

- ✦ evening events will remain every two months;
- ✦ they will be held on a Thursday;
- ✦ the start time will be 17.00 for coffee for a 17.30 start;
- ✦ the duration of the sessions will be of 1 ½ to 2 hours.

We will implement the slightly changed format beginning with the January 2001 meeting.
We are in the process of taking on board all your views, which will be reflected in next year's programme of events. By the time you read this, hopefully the programme of events for 2000/ 2001 will have been distributed.

As the year 2000 draws to a close, and the talk is all about the eEconomy and the Information Age, one old issue has raised its profile once more, that of software licensing. The anti-piracy groups Federation Against Software Theft (FAST) and the Business Software Alliance (BSA), amongst others, are becoming increasingly active in this area and some well known organisations have suffered public embarrassment, not to mention financial penalties. Many organisations still take the ostrich approach to this issue, and bury their heads in the sand. They see it as purely a compliance issue, they do not realise that there are real business benefits to be gained if they look at the wider issues and look at the whole concept of software asset management.

According to research by BSA, private copies of software accounted for 26% of all business applications sold in 1999 costing the software vendors approximately £457m in lost revenue.

The web currently serves as a black market for software pirates and this is likely to expand as bandwidth expands giving individuals the opportunity to download pirated applications on-line.

Figure 1. shows that the ability to download software from the internet will make the issue of ensuring compliance more difficult:

This is certainly something for IT Directors and Managers to consider when allowing employees access to the internet - limiting bandwidth may be an option.

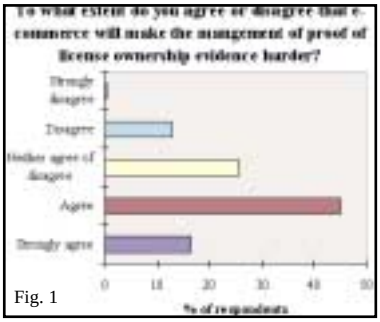


Fig. 1

Figure 2. shows that employees having access to the internet, and therefore the ability to download software, is wide spread:

According to research by industry analysts the Gartner Group, up to 30% of the cost of running PC's/servers can be saved after a software asset audit, reconciliation and inventory management process has been completed.

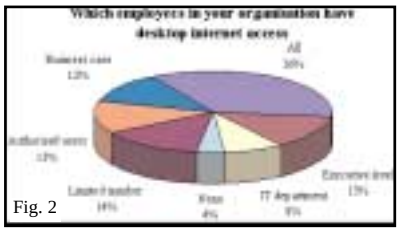


Fig. 2

FAST and KPMG's annual survey on software piracy amongst UK corporates has confirmed that software piracy is still not seen as an important issue. In addition UK corporate's are still unaware of the potential cost savings of becoming software compliant. The main findings show:

- ✦ Software licensing is still not being taken seriously by senior management (only 21% have board level responsibility, down from 30% last year). Yet it is found that more than 97% thought over half of the

software in the UK was illegal.

- ✦ Almost 50% of all organisations expect software received over the Internet in the coming year to increase. Linked with this, 60% believe that this will make proving ownership of software more difficult.
- ✦ 56% of respondents stated it would be difficult to prove ownership of all their software.
- ✦ 61% feel that the legal risk to their organisation of non-compliance was high.

Commenting on the main findings, Geoff Webster, CEO, FAST, said: "It is astonishing to see that board level executives are still not taking software piracy as an issue seriously. Surprisingly, large corporate's are still not getting the message that they can dramatically reduce the cost of ownership of their assets if they regain the loss of control."

He continued: "It seems that software piracy has become a side issue due to the rapid growth in the uptake of the Internet. If organisations are building new systems on the back of ones using illegal software, they really are putting their business operations at a massive risk. It would appear we still have a huge educational exercise to carry out in the marketplace. Over 2000 organisations are using the FAST programme to get control and there is no doubt that they are creating a real competitive edge over those who are ignoring the problem."

Paul Diamond, Director, KPMG, Information Risk Management Practice, said: "There must be a 'Win Win' opportunity for organisations in relation to this issue. We are talking about saving money and staying on the right side of the law. A company would not drive a fleet of stolen vehicles and this can be said the same for illegal software in an organisation. Private sector organisations such as retailers and banks take a dim view towards shoplifting and fraudulent use of their funds but yet do not appear to take using illegal software so seriously."

FAST noted that many senior managers in organisations do not recognise the benefits of an effective software management structure. Initially, the cost of implementing such processes may emerge high, however well managed software environments produce considerable monetary return within 12 months.

There are range of types of software piracy, the classifications are as follows:

Recordable CD-ROMs; This involves pirates compiling large amounts of software onto a recordable CD-ROM, making multiple copies of the CD-ROM, and selling to customers via different mediums, for example; 'Under the counter', mail order, retail outlets and markets. Pirate software is now advertised for sale on the internet and are usually publicized as fakes.

Professional Counterfeits; This software resembles the genuine article. The software is copied along with packages, licenses and holograms. Professional counterfeits are often produced to such a high quality, it can be difficult to distinguish between the real and fake item.

Hard Disk Loaders; This comprises of outlets or dealers loading versions of pirated software onto systems, encouraging customers to buy the hardware.

Corporate Over-Use; Software packages are installed on more machines within a company than the company holds licences for. If a company purchases 20 single user licenses for a software program and installs the software on 30 machines, 10 infringing copies are utilised. This is the same case for those running of networks.

Internet Piracy; This comprises of downloading or distributing software on the internet. Software can be present on internet sites however it is not necessarily legal or free for an individual to download. Various software is placed on the Internet without the copyright owners consent. Software pirates advertise their services on the Internet offering cheap mail order options. To establish the legal validity of the software on the internet, contact the software publisher directly.

This clearly shows there is an ever increasing number of entry points where illegal software may be introduced into an organisation, greatly increasing the risk that an organisation will be non-compliant.

What do you consider the legal risk to your organisation in failing to be software compliant to be?

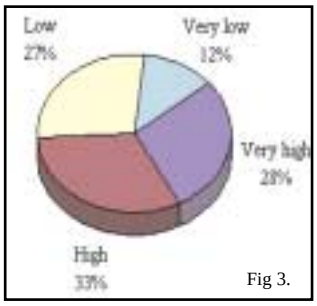


Fig 3.

Research suggests that the issue will continue to increase over the next few years. The Gartner Group predict that:

- ✦ through 2003 enterprises that fail to integrate software contract and inventory data to manage their software assets will overbuy licenses on 60% of their portfolio.
- ✦ through 2004, Gartner predict that enterprises that focus asset management efforts on collectively implementing process, people and technology improvements will experience annual per-seat savings of 20% to 40%.

So what can you as risk management professionals be doing? Well you could start by raising the issue with senior management within your oraganisation, and promoting the wider business benefits which can be achieved from a robust software asset management process.

You can start by considering the following questions:

- ✦ Do you have an accurate inventory of your IT assets including software?
- ✦ Do you have a process in place which enables you to track these assets on an on-going basis?
- ✦ Do you know how you can utilise this information to reduce costs and increase return on investment?
- ✦ Do you know how you can make better use of corporate procurement standards, saving time and money?
- ✦ Do you know how you can manage your IT Assets efficiently and effectively and obtain the optimal return on investment?

Northern News

By Ray Butler

Stop The Subversive Spreadsheet

The EuSpRIG (European Spreadsheet Risks Interest Group) symposium 'Spreadsheet Risks, Audit and Development methods' (sponsored by the Northern UK chapter) was a great success - More than 40 delegates - auditors, accountants, consultants from the Big 5, bankers and public sector managers as well as researchers from several universities, from 4 continents - attended.

Delegates were welcomed by Professor Brian Knight who gave a short history of the university campus, formerly the Royal Naval College, at which the event was being held. This was followed by a brief speech entitled 'Stop The Subversive Spreadsheet' in which Ray Butler, HM Customs & Excise and EuSpRIG Chairman, and David Chadwick, Symposium Organiser, described the factors that drove four people to meet for the first time in March 99 to found the group and begin preparations for a symposium. Ray concluded by welcoming

The first session 'Extent of the Problem: types of errors and risks' was chaired by somebody who had worked for more than fifteen years to raise awareness of spreadsheet risks throughout the world - Ray Panko of the University of Hawaii.

Prof. Panko gave a paper which immediately drew attention to the magnitude of the problem. He cited four major pieces of research since 1997 which used field audits of real business spreadsheets and which together gave an average error rate of 91% - an astoundingly high figure! He then discussed possible causes of such error-rates, common methods of error-prevention, detection and audit and their obvious and not-so-obvious shortcomings.

Pat Cleary, University of Wales, discussed his forthcoming research programme which will evaluate the importance of spreadsheets to organisations. Pat proposes to investigate several organisations in of health, retailing and public utilities. Many delegates expressed their support for this work and especially Ray Panko himself who stated that knowledge of the true reliance of organisations on their spreadsheets would give greater credence to public acceptance of the alarming data on error-rates. The first session was concluded with a paper by Kamalesen Rajalingham, a PhD student, who showed his comprehensive taxonomy of spreadsheet errors which he considered could classify any practical error found in the wild. The audience rose to this obvious challenge and presented Kamalesen with obscure practical error instances of their own daring him to classify them using his taxonomy. In each case he was successful.

Session two began with the chairperson Barry Pettifor, director of Spreadsheet Assurance Services at Pricewaterhouse Coopers, discussing the need for business and academia to explore better 'Development Methodologies and Techniques'. Barry then introduced Professor Brian Knight University of Greenwich who described a structured methodology for modelling spreadsheets developed by researchers at the Greenwich. Yirsaw Ayalew, of the University of Klagenfurt, Austria discussed his own methods of building and testing spreadsheet models beginning with the same software engineering approach as Brian knight but pointing out that although ' spreadsheets are software' there was the inherent problem that 'spreadsheet authors were not programmers'.

Leon Strous, of De Nederlandsche Bank in Amsterdam, chairing the third session 'Audit Methodologies and Techniques'. Ray Butler (H M Customs & Excise) described the risk assessment used by H M Customs & Excise for spreadsheet developments used for tax accounting.

Hoch Chuan Chan, of the University of Singapore, who demonstrated the difference between surface structure and deep structure in spreadsheet models, and the role of this difference as a cause of difficulty checking.

Lastly, Andrew Hawker (University of Birmingham), presented a short but interesting paper looking at the inherent problems associated with the use of the built-in accounting functions. Andrew drew attention to the difference in use of accounting functions in the UK and the USA and the confusion this could cause with products like Excel which were oriented to the American market. He also mentioned how novice spreadsheet users could be deluded by 'wizards' into thinking they had used a function correctly when in fact they had not. Interestingly, Andrew's paper was based on an article he had once published in the CASG Journal and which had caused some interest at the time.

The last session was devoted entirely to practical demonstrations of software tools particularly audit tools. James Sarmecanic of Operis demonstrated OAK (Operis Analysis Kit), Alastair Stewart & Ian James, of HM Customs and Excise, showed SpACE (SPreadsheet Audit for Customs & Excise). 'Spreadsheet Detective' was given a short demonstration by Dilwyn Edwards of the University of Greenwich.

The symposium rounded itself off with a panel of the four chairpersons fielding questions from the audience and opening discussion on how EuSpRIG should act to improve general awareness of spreadsheet risks, to develop research initiatives and to aid in setting standards of best-practice.

This produced lively discussion and a healthy atmosphere of differing opinions. The delegates concluded that the next conference should concentrate on best practice in model building and testing. Next year's EuSpRIG conference will be held in Amsterdam, and the Belux and Netherlands ISACA chapters have already offered their support.

To find out more about EuSpRIG visit the website (Conveniently linked to the ISACA Northern UK pages on www.isaca.org.uk) or email ray.butler@hmce.gov.uk Copies of the proceedings of the conference (a snip at £20 a copy) are available from EuSprig.

As president of the sponsoring ISACA Chapter it gave me great satisfaction to see so many professionals from so many business areas mingling with the academics to deal with a risk area that has bothered me for years.

Continued from page 9

Copyright can only be enforced territorially. In other words, the laws applicable to the country of origin protect copyright. With a UK based web site, the owner has recourse in law against anyone in the UK copying material from it. However, It is not possible to prevent anyone in China copying material, as UK law is not applicable.

The only exception to this is the 'Berne Copyright Convention'. The convention provides copyright protection within all signatory countries, (EU states, USA and Russia) provided that the copyright sign (a small 'c' within a circle) is displayed on the material.

As a general rule for Web sites it is not advisable to post any material for which copyright is an issue.

Trademarks

A trademark is defined as "any sign capable of being represented graphically which distinguishes the goods or services of one undertaking from those of another".

The logo of your company, and possibly the company name can be considered trademarks.

Trademark law is territorially enforced. Trademarks must be registered at a national level as there is no international registration agency (such as with patents). There are 42 classes of trademark which represent discrete industry groups. The word 'Macintosh' can be registered as a trademark for a computer in class 9 (electrical and scientific apparatus) and another company within the same geographical territory can register 'Macintosh' as a trademark for a raincoat in Class 25 (clothing). The trademarks can happily co-exist as under the law there as there is no possibility for confusion in the minds of consumers.

For the purposes of clarification, consider a hypothetical case. Assume that a financial services company in America starts an Internet bank called 'BankonLine' and registers the name as a trademark in the USA. The target market is the USA.

Through research, the company realises to its horror that there is another bank in Mexico called Bankonline which is available via the WWW to US customers. The US company starts a lawsuit against its Mexican namesake for 'infringement' of trademark. However, the Mexican bank has quite legitimately registered BankonLine as a trademark with the Mexican authorities. Its target market is Mexico not the US. The fact that the Web site may be viewed in the US is a characteristic of the WWW.

The US Company now faces the dilemma that if it launches an action for infringement it may provoke a reciprocal action from the Mexican bank for 'infringement' as the Web site of the US Bank is available to Mexican customers. Before the WWW both trademarks could have happily co-existed confined to their respective geographical territories. The problem with the WWW is that it instantly renders institutions 'global' because the sites are available to search engines used by consumers world-wide. This is a classic example of the law lagging behind technology.

Domain names

Assume that BankonLine reaches an amicable settlement with its Mexican counterpart. It must now turn to the issue of Domain name. An Internet Domain name, in law, is much more than an Internet address. It identifies an Internet site to those who reach it much like a company's name identifies a specific company.

If we come back to the Macintosh example mentioned earlier, while there could, theoretically be up to 42 'Macintosh' trademarks in the various industry classes, the nature of the Internet means that there can be only one 'Macintosh.com'

The US company registers BankonLine.com as its domain name. It now finds, during a Web Search, that a Canadian Bank has registered BankonLine.ca. The US bank is aggrieved and seeks recourse to legal counsel. The owner of BankonLine.ca is not registered in the US nor does it seek to sell its service in the US. The Web domain has been legitimately registered and the Canadian Bank has no office within the US. No Canadian law has been offended so the US Bank has no case.

The US Bank seeks recourse to the Internet Corporation for Assigned Names and Numbers (ICANN). However, it finds that the ICANN dispute policy applies only to generic top-level domain names and does not cover any domain name incorporating a country-code top level domain, (such as the 'dot ca' suffix). The argument here runs along the lines that a foreign trademark owner such as BankonLine in Canada has a legitimate interest in a domain name, which incorporates the country code of the country in which it is registered. Again the US Bank has no case.

'Cybersquatting' legislation does not apply in this case as the Canadian Bank has registered the domain name in good faith and has not registered the name with the intent of selling it on to the US Bank for profit. The only course open to the US Bank would be to purchase the domain name. This is likely to be expensive as the Domain name has been registered for an established e-business.

Could the US Bank have avoided the problem?

The only way of resolving the problem and gaining a global monopoly on the BankonLine domain name would be to register the name discretely in every country which has a country code top level domain. This is expensive, as there are 239 country code top-level domains.

This is not the end of the story. In each country there are a series of sub domains. The UK has .org, .co, .ltd, .plc, .net, .sch, .ac, .gov, .nhs, .police and .mod. The US bank would have to file over two thousand separate registrations to acquire all combinations of the domain name and in many countries, such as Canada, the registration of a Canadian country code sub domain to a company that is not federally incorporated within Canada is not permitted. Under Canadian law such a company is deemed to have no legitimate business interest in Canada.

In the unlikely event that

BankonLine.com is successful in registering all combinations of the domain name it is faced with a considerable ongoing expense. Domain name registrations, particularly for the all important '.com' suffix, are not granted in perpetuity. A regular maintenance fee will be payable to ensure continued ownership, the extent of the fee will depend upon the registration agency used.

The US Bank's troubles are not over, as well as the country code name dilemma, BankonLine has to contend with other domain names which include very similar names such as 'BonkonLine.com'. This turns out to be a salacious site. Porsche cars in the US recently launched an action against owners of Web sites with Porsche in the domain name, there were several hundred of these including 'PorscheGirls.com' all of which would be selected by any search engine in response to the input string of Porsche. This could result in customers having difficulty in identifying 'PorscheCarsUS' from the listing. The company claimed dilution of its trademark. The case was unsuccessful.

Legal liability and hypertext linking

This issue was raised in two recent cases, the first in the UK involving the Shetland Times, Jonathan Wills and Zetnews and the second in the US involving the Washington Post and TotalNews.

In the UK case the Shetland News set up a Web site that included headlines copied from its competitor the Shetland Times. When a user visited the Shetland News Website and clicked on a headline, a hypertext link transferred the user to the Shetland Times site where the article was displayed. The Shetland Times successfully made a case in court that this breached their copyright and misled users into thinking that the articles were part of the Shetland News.

In the US case, TotalNews, an aggregator of Web news stories, employed frame technology to display news sites from around the world. When a user clicked on the news source (e.g. Yahoo! News, BBC online or ABC Radio), the content from the news source filled the frame. However, the frame was surrounded by TotalNews's URL, banners and advertising. Six of the content providers involved sued claiming that the use of framing was the Internet equivalent of pirating copyright material. The content providers were highly motivated to sue as all made revenue from advertisements on their Web sites, the amount of which depended upon the traffic they generated and by using framing technology, TotalNews was preventing the display of the advertisements. The case was eventually settled out of court for an undisclosed sum.

Interestingly enough, the content providers concerned provided a license for TotalNews to link to their Websites via hypertext links. The case therefore centered upon the use of framing technology and the issue of 'commercial fair play' rather than the issue of whether TotalNews could link if the content providers refused to consent to the link.

The issue on the legality of linking depends upon the concept of 'commercial fair play' and 'reasonable expectation of privacy'. The concept of 'commercial fair play' centres upon whether a company has unfairly exploited the content and work of another linked party and has unfairly benefited from the work of the content provider. Framing technology in particular, can mislead a user into believing that a commercial relationship between two organisations exists, when it does not and could be regarded by the courts as breaching the principle of 'commercial fair play'.

The principle of 'reasonable expectation of privacy' can best be illustrated by example. Assume that someone walks down the middle of a busy shopping arcade holding up a sign which says 'don't look at me' can they sue somebody who happens to look their way? The law in most countries says that they could not because there was no 'reasonable expectation of privacy'. Similarly, by setting up a Website on the WWW, there can be no 'reasonable expectation of privacy', even if the site declares as much. The legal principles applying to the WWW are the same as those applying to non-Web activity. Under these principles a shop cannot enforce a billboard outside it's premises declaring 'don't include this shop in tourist guides' Similarly, anyone can set up a Web site and declare that 'these are the 10 most useless sites on the Web' and provide links to them, (in fact there is such a site which lists 'Web pages that suck'- check that your company isn't listed!) The only occasion where a link may fall foul of the 'reasonable expectation of privacy' principle is where the link circumvents an access control mechanism designed to restrict parts of the site to members of an organisation or subscribers to a service.

Linking is essentially the essence of the WWW and search engines such as Alta Vista or Exite! could not operate without this ability. Linking without consent on the WWW is entirely legal. Linking is only considered illegal if it violates a trademark or copyright, is defamatory or breaches the principles of 'commercial fair play' or 'reasonable expectation of privacy'. Links that could violate 'commercial fair play' and the 'reasonable expectations of privacy principles' fall into the following categories:

- where the link uses a trademark or logo of the linked site
- where there is 'deep linking' to an internal page which circumvents the sites disclaimers or terms and conditions statements (under most legal conventions stores have a right to require you to enter via the front door and ensure that you pass by all the dump bins full of impulse purchases) or links to pages reserved for members which require a password to access where the frame modifies or distorts the linked site
- where the link implies an endorsement or an affiliation which does not exist
- 'IMG linking' (where the link uses an image imported from the site and therefore breaches copyright).

There are forms of linking which inhabit a 'grey area'of the law. These are not technically illegal but could well provoke legal action from an aggrieved party:

- ✦ where the linked site expressly requires consent
- ✦ where the link diverts traffic from the Web site and reduces advertising revenue.

Legal Issues associated with Metatags

The use and abuse of metatags has been subject to case law in the US over the past three years. In June 2000 case law on this issue was established in the UK. The issues arising relate to trademark and copyright infringement but are worth mentioning in their own right.

Metatags consist of HTML code inserted into a website by the owner. They comprise of keywords and phrases which describe the content of the website and are ignored by Internet Browsers when interpreting the graphical and textual elements of a Web page. However, metatags are invaluable to Internet Search engine 'spyders 'which use the Website metatags to categorise the site for listing in responses to user defined searches.

In addition to categorising a site, the content of a Metatag is frequently used by search engines to determine the priority of the site within a search list. High priority sites are closer to the top of the list. A commercial site, which gains revenue either from sales of products or services or from the amount of traffic it generates, in terms of the number of people who view it's advertising banners, has a high incentive to be listed as close to the top of any search list as possible because users normally visit only the sites near the top of the list.

Unscrupulous sites may also have an incentive to 'spoof' by creating inaccurate metatags. Let us return to the example of 'BankonLine.com', which, has successfully registered its domain name but is finding that the traffic to the part of its Web site selling investment products is poor. The Investment Product Manager has targets to meet and notices that BigBank. is receiving a large number of 'hits'. He persuades the Web Site Content Manager to change the Metatag for 'BankonLine.com' to read 'BigBank BigBank BigBank'. Web search engine 'spyders' reading the Metatag will now list the site for any searches conducted by customers on BigBank and because of the way in which the Metatag has been constructed, the site will appear high in the search list. Any customers searching for BigBank investment products who happen to select the link will now be routed to the BankonLine.com. BigBank may lose potential customers to Bankon-Line.com

A situation could also exist where potential customers could be routed to salacious sites or sites established by a discontented customer who may bear a grudge against BigBank.

Case law in the US over the past three years has established precedents for legal action. In 1997, in the state of Colorado, a court found that 'Advanced Concepts' had unlawfully included metatags for the legal firm of 'Oppedahl and Larson' in its site. The legal firm specialised in domain name disputes and the court found that Advanced Concepts had no reason to include the name of the firm in its metatags other than to capture traffic that would gain them domain name registration fees or web site hosting clients. Similarly, In 1998 a Virginia court in Playboy vs Asia Focus International awarded $3m plus costs and attorneys' fees as recompense to PEI (the owners of Playboy) for infringement by Asia Focus International of the Playboy and Playmate trademarks. The trademarks had been incorporated into the domain names and metatags of Asia Focus International sites with the intention of misleading customers.

The growth of legal cases involving the use metatags being brought before the US courts resulted in a ruling on 22 April 1999 by the 9th US District Court of Appeals banning the use of unauthorised trademarks within a Metatag (Brookfield Communication Inc vs West Coast Entertainment Corporation). This ruling was based upon a new legal concept of 'initial interest confusion' established for Metatag cases. It is binding in California and eight other US States.

In June 2000, the UK High Court ruled against a computer company called Mandata, ordering it to pay damages to Road Track Computer Systems. Mandata had used metatags to divert Internet traffic from the web site of its rival and that and according to the Court this constituted a "blatant and unsophisticated infringement" of Road Track's Intellectual property rights. The court found that the use of a rival's mark in metatags where the sole purpose was to divert Internet traffic from that company's site amounted to a trademark infringement in 'passing off'.

The High Court's ruling in this case is a summary judgment so that it does not set a legal precedent but it does serve to illustrate that the UK is likely to follow the USA in discouraging the use of trademarks in this way.

Regulatory Issues Associated with Linking

In addition to the legal concerns mentioned above, Financial Service organisations have additional issues to consider. The advice provided by the FSA Internet Unit is that regulatory issues will arise in two ways. Firstly if the link goes beyond the bare name or icon of the site to which the link is directed and includes advertising material which appears to provide financial guidance (e.g. "XYZ is best for investment advice"). These words would constitute a financial advertisement and would need to be issued or approved by an authorised person. Secondly, a firm which establishing even a bare link will need to be careful that the site to which it is linked does not contain material amounting to an unlawful promotion. In the eyes of the regulator such a link will have 'caused' an unlawful financial promotion to be communicated.

The FSA requires 'due diligence' to be followed in establishing links. This could extend beyond researching the site prior to linking to putting a process in place for ensuring the linked site remains compliant.

Legal liability for the content on a linked site

If we assume that the BankonLine site has a link to a third party site which has inadvertently breached copyright. Could BankonLine be liable?

YOUR LETTERS

Information Content of Web Pages

Our committee is undoubtedly wise as you point out in 'The Editor's Chair'. However, on the subject of putting the content of DataWatch on line, I'm not convinced by the argument. Although the Datawatch magazine is paid for by our subscriptions, to not put the content on the web site because somehow we would 'lose the benefit' seems to me to run counter to the nature and economy of the web.

We, a community seeking to improve IT governance, security and control, and measures such as making good guidance publicly available are likely to grow the community and improve its collective knowledge and value which is in all of our interests.

Are we really likely to see displacement? Will members cease to pay their dues (or non-members not sign up) if they can get just one of the many benefits of membership in a comparatively inconvenient form? We can take a leaf out of the book of ISACA themselves. While the whole CobiT is priced at $70.00, most of it is available on-line. Why should this be?

1 Well, how usable is it on line? There is evidence that users will read only about two screens of material before they click off.
2 The bit that you want to use is not free. An analogy might be buying a kettle without a lead.

You could regard the freely accessible elements as 'free samples' in a difficult to use form. Making the content publicly available enables us to use the content to attract and capture additional members. Since the expensive work in writing the content and publishing it has already been done, the marginal cost of putting it on line is minimal, making this a low cost but high value means of spreading the good IT governance message and of attracting new members.

Other things could be done to differentiate the value between non-members and members. If non-members could only get this quarter's articles, members could (as you suggested in July-August 2000) have a private area with a searchable archive. Then the member gets his value while the non-member sees a differentiation worth paying a premium for.

Registration could be a powerful tool as well. If non-members wish to access a sub-set of what we make available to members only, say one year's worth of the archive or the bulletin board, we could capture personal details and use this information to target potential additional members.

Andrew Shefford
by email

Andrew,

Thanks you for your comments regarding publishing the contents of Datawatch on the web. You are not the first to suggest that the publication should be made available online and the Committee has been debating this issue for some time.

I share your views that making good guidance publicly available is of value to us all and you will therefore be pleased to see that Datawatch articles are now available to all visitors to the site. However, to ensure that members enjoy some privileges, articles from a particular edition will only appear on the site once the newer edition of Datawatch is published.

The Committee has also been talking about providing an area on the web that is restricted to members, along the lines of the main ISACA website. However, this will require some form of registration, and currently it is not a route we particularly want to go down as we don't wish to have to collect and maintain any personal data on the website. An alternative would be to provide a generic key (password) that would not generally be available to non members, for example by publishing it in Datawatch. A decision has not yet been reached on the members restricted area, so if you, or indeed any members reading this have any suggestions, please let us know.

Allan Boardman, Webmaster

Continued from page 27

It was once theorised by a European mathematician that anyone in the world could be linked to anyone else by six degrees of separation. I have a friend who knows somebody who has a brother, who has a cousin in the US whose brother works in the Whitehouse and knows Bill Clinton (I seem to remember that there was a Hollywood film starring Donald Sutherland a couple of years ago based upon this proposition). If this is theoretically true of human beings it is literally true on the WWW. Links interconnect sites on the Web like neurons in a human brain. If the principle of liability by association were to be applied, virtually every site owner on the Web would be liable for copyright infringement as somewhere within the chain of interconnecting of links there would be an 'infringing' site. The only exception is the regulatory situation mentioned above in the context of unlawful financial promotions but it is unlikely that this would extend beyond the immediate linking association provided that due diligence in linking can be demonstrated. However, for safety reasons it is advisable to post a disclaimer on the site indicating that links are for informational purposes only and do not constitute an endorsement or approval of the material on the site.

The second half of this article will be published in the next edition of Datawatch and will cover the OECD Guidelines on Data Protection, cross border data flows, legal issues associated with the use of 'cookies', defamation on the Internet, the implications of the Human Rights Act for the monitoring of employee e-mail use, bulletin boards and the legal admissibility of electronic evidence.