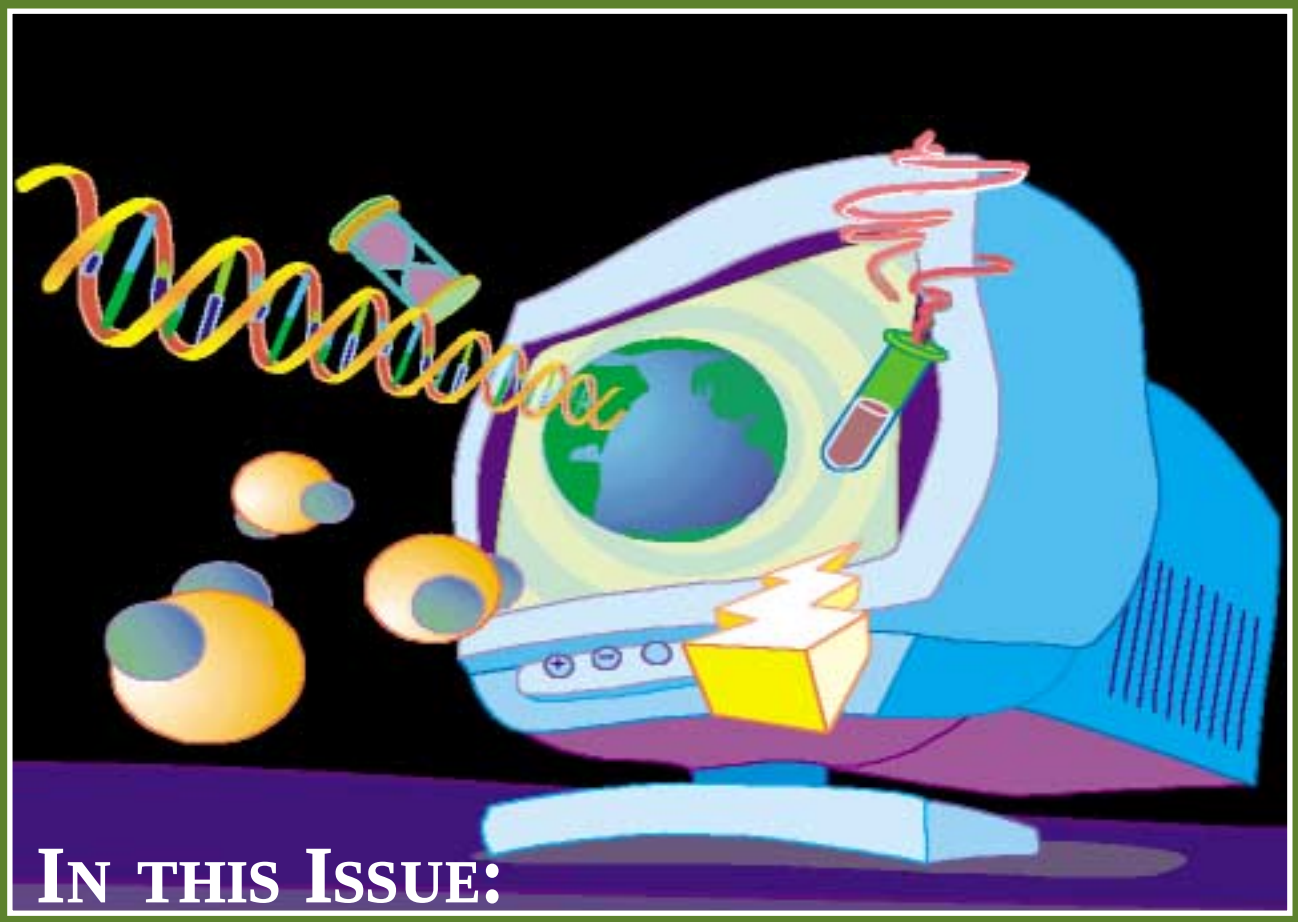
ISSN 1356-0735

London Chapter's 20th Anniversary

DATAWATCH

Vol. 47, Jan-Mar 2001



In this Issue:

The 'E-Corporation' & the Law

NT's Ultimate Countermeasure

The Quarterly Magazine of ISACA London Chapter

VOLUME 47 JAN-MAR 2001

DATAWATCH

is a quarterly magazine published by the

Information Systems Audit and Control Association

London Chapter

Chapter Office:
10 Drayhorse Road
Ramsey, Huntingdon
Cambs PE26 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

Hello and welcome to the first Datawatch edition of 2001.

Will it be an audit odyssey I ask myself, or are we all fed up with jokes on those lines already?? At least it was a quieter one for most of us than the advent of the year 2000 was.

If I had a crystal ball then I might be tempted to try it out to see what 2001 might bring to audit agendas. It looks as if e-commerce is still going to be a hot topic one way or another, whether through success or failure, but I'm sure many of us are going to be involved in our employers' activities in this area, whether it's B2B, B2C, etc. This edition sees the second half of Andy Farrington's article on the legal aspects of e-commerce for those of you following this series.

Bill Hawkins, who provides library liaison for the Chapter as well as being on the Editorial team, has provided an article about the Chapter Library, held in the Guildhall in London. It's more of an historical collection than current material, so can I draw your attention to Bill's request for any books on computing or computer audit that you might consider outdated? Rather than throwing them away they could form a useful part of the collection. Refer to Bill's article for more information if you have anything you think might be appropriate.

If like me you are already counting the cost of Christmas and have already offered to wash your boss's car in anticipation of favours required in the next round of pay increases (or otherwise), you may find Adrian Simpson's article timely in which he talks through some of the results of a recent survey of computer auditors carried out on the subject of staying put or moving on in the job market. If one of your New Year's resolutions fell into this category, read on!

And don't forget to take a look at the Chapter web site if you haven't done so recently - there are some new categorised discussion forums for members to use, so feel free to make use of them!

Best wishes for a happy and prosperous 2001 from all the editorial team!

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

The theme for the current season is e-business and the risks associated with that form of trading are being raised by our various speakers. What I am noticing is that e-business risks are slightly, but not totally different, from risks associated with any business which relies on information technology to support its business objectives. In the case of e-business however, the reliance on technology is total and the interface with the customer is direct. This means that the customer is instantly aware of any shortcomings in the service and his/her perceptions of the company are often formed in the first few seconds at the company's site. However, it is rare that the service you are providing is totally within your control. Most companies rely on partners to provide their web presence. Thus your customers perception of your company may depend on third parties. What do you know about them, and their own service providers and what contracts and service level agreements do you have in place?

There are three traditional concerns that need to be examined when providing a web based interface to your customers, or business partners. These are confidentiality, integrity and availability. How certain are you that your company's information can only be accessed by authorised users via the company's web site? How certain are you that customer information can only be accessed by the customer concerned? What contingency plans do you have to deal with a breach of confidentiality? How certain are you that the information displayed on your web site is accurate? In the event of the displayed data being incorrect, or becoming corrupted, how soon would you know about it? Will this be before the media find out? What contingency plans do you have to deal with a breach of integrity? How certain are you that your company's web site will be accessible to your customers? In the event of the site being inaccessible, how soon would you know about it? What contingency plans do you have to deal with a loss of accessibility?

All of the above are potentially bad for your company's reputation, but what would be worse is for your site to be defaced. This sends a message to world that your security is poor and therefore your customers' data is insecure. E-business puts you in touch with your customers. It also makes your weaknesses more apparent. Design with security and maintenance in mind. Know your partners really well and remember that a web site is for life and not just for now.

Happy Anniversary 20 London Chapter

This year sees London Chapter celebrates its 20th year since formation.

We've come a long way since 1981, as has our industry. New risks have arisen, new responsibilities are there to be grasped and London Chapter has grown to be the second largest in the world.

Membership in 1981 was under 30; in 1991 it was 230! At the beginning of 2001, 730! A quite remarkable growth that we can be proud of.

Thanks must go to the numerous individuals who have served the London Chapter over the past 20 years. We are hoping to bring you more details of these stalwarts over the next few issues of Datawatch.

Thanks must also go to all the companies that have supported the chapter. Whether it be hosting chapter meetings, committee meetings, SIG meetings, workshops, social events or just by allowing their staff time to take part.

Some of the membership will remember the 20th anniversary celebrations: a dinner held on November 19 1991 at the Cafe Royal. The Cafe Royal was specifically chosen because that was where the inaugural meeting was held back in 1981. Of course, we will not allow the 20th anniversary to go by unmarked and further details of the committee's plans will be published soon.

Information Systems Audit and Control Association

The 'E-Corporation' and the Law

By Andy Farrington

This concludes the article on e-commerce law, the first part of which was published in Datawatch edition 46

The views expressed within this article are entirely those of the author and do not necessarily reflect the views of ISACA, ISACA London Chapter or the author's employer. ISACA, ISACA London Chapter and the author's employer take no responsibility for losses, difficulties encountered or consequences arising from actions taken by any party as a result of information contained within the article.

PRIVACY AND DATA PROTECTION

OECD Guidelines on Data Privacy

In 1980 the General Council of the OECD (Organisation for Economic Co-operation and Development) which represents 29 countries around the World, approved a series of guidelines on the protection of privacy and the transborder flows of personal data.

The guidelines set out eight general principles, which were designed for member states to incorporate within national legislation.

- **The Collection Limitation Principle:** which requires limits to be placed on the collection of personal data and that any personal data should be obtained by lawful and fair means and the knowledge of the data subject.

- **The Data Quality Principle**: which requires data, to be accurate, complete and kept up to date.

- **The Purpose Specification Principle:** which requires that the purposes for which personal data are collected should be specified not later than the time of data collection and that subsequent use is limited to the fulfilment of those purposes or to purposes which are not incompatible.

- **The Use Limitation Principle:** which requires that data should not be disclosed, used or made available for purposes other than those for which it has been collected.

- **The Security Safeguards Principle:** which requires that personal data should be protected by reasonable security safeguards.

- **The Openness Principle:** which requires companies collecting personal data to operate a general policy of openness about developments, practices and policies with respect to personal data.

- **The Individual Participation Principle:** which requires that arrangements be made to allow individuals to exercise a right of access to personal data held on them.

- **The Accountability Principle:** which requires that a data controller be appointed to ensure compliance with the principles.

If the Principles look familiar, it is because they have formed the framework for the EU Data Protection Directive as well as data protection law in the 29 member countries of the OECD.

Cross Border Data Flows

Data protection laws are territorially defined. Complications exist when personal data on individuals, who are citizens of countries which have data protection legislation, is sent for storage or processing to countries which have no such legislation.

A good example of this is the EU which places an obligation on member states to ensure that any personal data transferred out of an EU country is 'adequately protected'

The European Commission has the right to determine whether a country has an 'adequate level of protection'. A country which does not have data protection legislation cannot be considered to have 'adequate protection' and the transfer of personal data is prohibited.

Until recently this issue has created an 'impasse' for countries in the EU which have close economic links with the USA as the latter has no data protection legislation.

Following two years of discussion with the US State Department, a resolution was proposed called the 'Safe Harbour Principle' which allows the EU Commission to regard data transfers to the US as offering

'adequate protection' under EU legislation.

Under the arrangement, the US Department of Commerce will establish a list of US companies adhering to data protection rules which the EU Commission regards as offering 'adequate protection'. Companies within the US, which appear on the list 'bind themselves' publicly to the Safe Harbour Principle. Compliance will be checked by US authorities and non-compliance will be subject to legal sanctions under the US Federal Trade Commission Act which forbids misrepresentation and deceptive trade practices.

The extent to which this problem can be considered to be resolved is a matter of debate at the time of writing. On 5th July 2000 the EU Parliament voted to accept a report produced by Italian MEP Elena Ornella Paciotti calling on the EU Commission to reopen the Safe Harbour negotiations and to stop all EU-US data exchanges under the principle until it can be verified that the companies listed have made adequate arrangements to comply with all the provisions of the EU Data Protection Directive.

The legality of Cookies

A 'cookie' is a small piece of information sent by a web server for storage on the machine hosting the web browser so it can later be read back from that browser. This is a useful technique for having the browser remember some specific information.

An example of a 'cookie' is when a browser stores an individual's passwords and user ID's. 'Cookies' can also be used to store the preferences of start pages. Both Microsoft and Netscape use 'cookies' to create personal start pages. The most common uses to which 'cookies' are put are listed below.

On-line Ordering Systems.

'Cookies' can be programmed to remember what a customer wants to buy. If a customer is disconnected from the ISP during an online transaction the session can be resumed without having to reselect items which have already been chosen. This technique is used by many B2C retailers.

Site Personalisation.

This allows a subscriber to a particular service to personalise the service they receive. A 'cookie' could be used by a News aggregator on the Web to hold details of a subscriber's personal news preferences and to filter out inappropriate information.

Website Tracking.

This enables a web site owner to see what interests an individual who is browsing the site. For an online retailer it helps to identify the type of product lines customers are interested in and also gives information on the navigability of the site. There may be parts of the site which are never visited or where the navigation is unwieldy causing potential customers to abandon attempts to browse the page. It can also provide accurate information on flows of people to the site, particularly those who have returned.

Targeted Marketing.

This is one of the main uses of cookies. The 'cookie' can be used to build up a profile of where a customer goes and what adverts they click on. This information is then used to target adverts at them, which the site owner thinks will be of interest. Companies also use cookies to store details of adverts which have been displayed so the same advert does not get displayed twice

User ID's.

'Cookies' can be used to hold User Ids.

'Cookies' are legal but this may not continue to be the case as the use of cookies as a way of collecting information about customers could be facing legal challenges in the near future.

A class action has been filed in the US against a company called DoubleClick. The lawsuit alleges that DoubleClick employs Internet 'cookies' to identify users and track their movements on the Internet. The company tracks and records the sites an individual visits, as well as the information transmitted on the sites, such as names, ages, addresses, shopping patterns and financial information. The suit alleges that after DoubleClick's purchase of direct marketing firm 'Abacus Direct' in 1998, it combined the cookie technology with other information it had acquired, in order to cross-reference personal information without the consent or knowledge of users.

In a similar case a company called 'Real Networks' has recently come under fire for using cookies to gather personal information about the musical tastes of users of the company's RealJukebox' software, which lets users download digital music files from the WWW. There are allegations that the company sold the information to third parties to use in targeted marketing campaigns.

There is increasing debate among privacy groups on the Internet concerning the use of 'cookies'. There is currently a risk that any use of 'cookies' by an organisation, which is perceived to compromise personal privacy, particularly in the context of marketing, could face unwelcome publicity and possibly legal challenge.

DEFAMATION

Defamation can be defined as the publication of a false statement which harms the reputation of another individual, group or organisation. Written defamation is called libel and oral defamation is called slander.

One of the most important principles in considering this issue is that of 'vicarious liability'. This legal principle is found in most judicial frameworks around the

World. Vicarious liability is the single most important legal underpinning for liability on the Internet as it makes employers liable for the actions of their employees. It is an outgrowth of the legal doctrine that a parent is responsible for the acts of their children. The presumption in each case is that the parent, or employer, has the duty and ability to control the wrongdoer, so that when the wrongdoer injures another, it is the employer, or the parent, who is sued. The principle finds liability even when the defendant (the parent or employer) has done nothing wrong, and was unaware of the wrongdoing. A large variety of wrongs are subject to vicarious liability: copyright and trademark infringement, harassment, discrimination, and so on.

The principle can extend to defamation in that if an email containing defamatory statements is sent from an employers premises, the employer could be held liable.

It is important to appreciate that this principle is not restricted to e-mail sent outside the company. In the eyes of the law there is no differentiation between an internal and external e-mail in terms of defamation.

This is illustrated by the case of Norwich Union (NU), a UK based Insurance Company. In 1995 an employee of Norwich Union sent an email to another employee which depicted the financial situation of the Western Provident Association, as being far worse than it actually was. Western Provident heard that such an email was circulating and obtained an order from the court to search the hard drives of the NU e-mail system. The incriminating email was recovered and Western Provident sued Norwich Union in the first corporate libel by e-mail case in the UK. Norwich Union lost the case, had to make a public apology and paid Western Provident £450,000 in costs and damages.

In a similar case a customer took legal action against a large UK supermarket chain called ASDA (which has recently been bought by the US Wal-Mart Group). A UK police officer obtained a refund from the supermarket following a complaint about the quality of the produce he had purchased. The staff, however, wrongly believed that he had been practising a refund 'scam' and promptly posted a message onto the ASDA e-mail system, copying it to all ASDA branches in the area. The message informed staff to watch out for the man and gave a full physical description. After visiting a local ASDA store a few weeks later in his capacity as a police officer, a member of staff alerted him to the message which he promptly read. ASDA reached an out of court settlement of £10,000.

Before the advent of e-mail this case would probably have remained slander within the local store, but the circulation of an e-mail throughout the company premises resulted in it being a much more serious matter.

Vicarious liability is not restricted to email, it can occur with any form of electronic 'publication' such as text on web pages, postings to bulletin boards and files made available for downloading. For example, an employees can infringe copyright on the Internet by forwarding e-mails with infringing attachments, or by copying and downloading material (including computer programs, screen savers, sounds and images) that are subject to copyright protection.

E-mail correspondence can also create problems for contractual arrangements by its very informality. If pre-contractual negotiations are conducted between customers and sales staff, there is a risk of pre-contractual misrepresentation with staff sometimes making statements which can give rise to problems at a later date. This issue not unique to email in that the same problems can arise with the telephone or face to face negotiation. This is normally overcome via the contract including a small print provision which expressly limits the contractual terms to those contained in the written document. The legal status of 'verbal' agreements or telephone discussions have always been questionable in terms of them being one person's word against another. E-mail changes this in that there may be a record of written statements, which, under E-commerce legislation, may become legally admissible as evidence in any legal dispute.

The relative informality and ease of use of email can result in employees breaching anti-discrimination legislation. There have been numerous cases in the US of sexist Internet jokes being circulated via email being successfully used in pursuit of sexual harassment cases. The same issue applies to racial discrimination.

Again, the principle of vicarious liability could result in employers facing prosecution rather than individual members of staff.

Monitoring of employee e-mail

One solution to the problem of vicarious liability is to routinely monitor employee e-mail communications to ensure that potentially defamatory statements are intercepted before they reach their intended source.

Under UK law, the interception of telephone calls (and by extension e-mail communications) is subject to the Interception of Communications Act 1985. This covers all calls made on public lines but not on private networks. The absence of a statutory framework for private telephone systems has meant that historically an employee had little redress if an employer has conducted covert surveillance by tapping a line on the private side of the network. This situation is now about to change.

The legality of employer interception was thrown into doubt

by the case of Alison Halford, a former Assistant Chief Constable with the UK Merseyside Police. Halford complained that following the start of her sex discrimination case against the police, her office telephone had been 'bugged'. While the British Government asserted that this was not illegal as the Interception of Communications Act did not apply to employers, Halford maintained that the absence of a legal framework within the UK for interception on private networks breached Article 8(1) of the European Convention on Human Rights (ECHR) which relates to her right of privacy. Furthermore the absence of such a framework meant that there was no right of redress , breaching her rights under Article 13 of the Convention. Her appeal to the European Court of Human Rights was successful. The court ruled that the absence of a statutory framework in the UK for interception on private networks contravened both articles 8 and 13 of the Convention.

The response of the UK Government to its defeat on this issue was published in the consultation paper 'Interception of Communication in the United Kingdom' The current proposal is to implement the Halford judgement by extending the interception regime to all telecommunications networks, whether public or private. This means that potentially any interception can fall within the scope of article 8 and that a single framework will now exist for all forms of lawful interception. The provisions of the Regulation of Investigatory Powers Bill, (RIP) currently before Parliament will be to extend and regulate the warranted interception regime which will address the deficiencies in the regulatory regime noted in the Halford judgement. It also addresses the EU Telecoms Data Protection Directive which includes a provision, under section 14(1,) requiring member states to prohibit interception of telecommunications services without the consent of users unless specific legal authority is given to do so. This in turn must accord with the Human Rights Act in the UK

The Regulation of Investigatory Powers Bill, (which received Royal Assent on 28th July and which, by the time you read this, may be law), could have an impact upon all forms of telecommunications interception conducted by companies, including the monitoring of employees. The text of the Bill, as it stands appears quite 'draconian' but the intention is to moderate the interpretation of the Act through codes of practice. For example, the government states that it is not the intention of the Act to impede the monitoring of communications by employers when such monitoring is conducted in the course of 'lawful business practice 'and (this is a crucial point) where the system operator has taken reasonable steps to inform the parties to the communication that it may occur. The question, however, remains as what the courts may interpret to be 'lawful business practice'

The draft code of practice for the RIP bill was made available on the DTI Web site from the end of July 2000 and, at the time of writing was available for discussion. The code permits interception without consent for 'lawful business practice' in the following circumstances;

- ✦ Providing evidence of a commercial transaction
- ✦ Providing evidence of other business communications to establish facts or ascertain compliance with regulatory practices or procedures
- ✦ Audit
- ✦ Debt recovery
- ✦ Dispute resolution

Interception for anything other than the reasons detailed above will be unlawful unless consent is provided. This may be in the form of written consent or a contractual condition of employment. Implied consent may be sufficient but if reliance is placed on this the policy must be sufficiently well advertised to ensure that it is known to all employees who may be affected. . It should be noted however, that 'obtaining consent' might be insufficient to escape liability. Article 8 of the Convention acknowledges a right of privacy in private family life and associated correspondence. There is an implicit acknowledgement that it is not reasonable to expect that employees will never be contacted at work on these issues. So monitoring, even with consent, could be held to be illegal if there is no alternative means of communication provided by the employer. One way around this would be to ensure sufficient provision of unmonitored payphones for employees to use.

In the UK the Human Rights Act received Royal Assent in 1998 and is due to complete is passage into law by October 2000. The Act incorporates the articles established in the European Convention on Human Rights. This will make it much easier to progress breaches of personal privacy through the UK courts. Once the RIP and Human Rights Acts are in force it may well be that a number of UK companies find that their current policies on the interception of staff telecommunications are illegal. In fact, in the light of the Halsted case, many companies in the UK may already be operating policies open to legal challenge.

This view is reinforced in a report by Robin Chater of Privacy International which was commissioned in September 1999 by the Office of the Data Protection Registrar in the UK. The objective of the report was to look at the misuse of personal data at work. The report found that currently employers in the UK who routinely monitor their employees could easily find themselves in breach of ECHR. The report also goes on to

suggest that government interception, as a whole will need to be reconsidered when the UK introduces the Human Rights Act. (the potential conflict between some aspects of the RIP and the Human Rights Act may result in some interesting legal cases.).

In the USA there is a principle of privacy whereby an individual can expect "reasonable expectation of privacy in Internet use". This is important, as it is possible that a court faced with an appropriate set of facts could find against an employer for breach of this privacy right. In the case of O'Connor v Ortega, the U.S. Supreme Court held, that a doctor at a State hospital had a reasonable expectation of privacy in his desk and file cabinet areas which were off limits to other hospital workers. This reasoning is applicable to electronic files kept on a hard drive under certain circumstances e.g. employer monitoring of employee e-mail stored locally.

To conclude, It is possible that monitoring of e-mail use by employers could be constrained in any country, which has enacted human rights or privacy legislation.

The Bulletin Board Issue

Internet sharedealing is experiencing an unprecedented level of growth throughout the world. Keeping pace with this growth are the number of finance related Bulletin Board sites. 'Motley Fool' and 'Hemmington-Scott' are two of the best known but companies such as 'Yahoo!' are also offering such services via their portal.

Finance related bulletin boards are hotbeds of legal action at the moment. The bulletin boards allow free ranging comment about companies and their financial prospects ranging from stinging barbs about the CEO to diatribes about business decisions. Many companies are taking exception to the nature of some postings, fearful of the possible effect that a rumour can have on a company's share price or incensed at highly critical comments of the senior management.

Particular concerns centre upon anonymous posting that some companies believe to have originated from employees.

In July 2000 Credit Suisse First Boston launched a lawsuit against 'Yahoo!' asked for $1m in damages from a group of message posters who allegedly libelled and defamed the firm by making derogatory comments about the company on a bulletin board. 'Yahoo!', as the site host, is being pressed to reveal the names of the posters.

The computer database company 'Informix' has started legal proceedings claiming that an insider leaked confidential information anonymously to a financial bulletin board claiming that its annual results would be weaker than expected.

Note: Yahoo is now receiving subpoenas to reveal the names of anonymous posters on a regular basis . During 1999 the American company Raytheon issues over 21 subpoenas to Yahoo related to bulletin board postings. There is evidence that US companies are increasingly turning to litigation as a means of suppressing any form of negative posting, as actions are not currently being confined to postings, which are obviously 'defamatory' or publicise 'confidential' information.

Just to prove that no matter what you do you can't win, 'Yahoo!' is currently being sued by a an anonymous message poster claiming that the company breached the First Amendment to the US Constitution in handing over his name to a company that is now suing him for a statement made about the company on a financial bulletin board. The lawsuit seeks 'punitive and unspecified 'damages against 'Yahoo!'.

The other issue surrounding financial bulletin boards is that of market manipulation. Under the protection of anonymous posting, individuals, companies and institutions can seek to influence share prices by 'hyping' a poorly performing share to encourage investors to purchase thereby artificially driving up the price. When the price reaches the desired level the perpetrator sells, leaving those who fell for the 'hype' to watch the value of their 'investment' plummet. This practice is called 'ramping' when it occurs on the Internet and appears to be a variation on the 'boiler room' scams common in the US in the 1980s. This issue has been a matter of considerable concern for the SEC in the US and the FSA in the UK.

The case of Lawrence Godfrey vs Demon Internet in 1999 brought case law to the UK. An anonymous person "posted" information about Godfrey, who was a university lecturer, on a Demon Internet hosted newsgroup. Godfrey told Demon about the information, informing them that it was untrue and defamatory. Demon did nothing about it. The Judge decided that as from the date Demon knew of the defamatory content of the material they were liable to Godfrey. Demon had hoped that they would win the action as cases in America have indicated ISPs should not be liable in these circumstances. This decision clearly puts ISPs in a difficult position. If someone complains that material published about them is defamatory then the ISP runs the risk of being successfully sued if they do not remove the material from their computers.

LEGAL ADMISSIBILITY OF ELECTRONIC EVIDENCE.

E- Commerce enabling legislation introduced by many countries under the UNICITRAL model Law (mentioned previously) has done a great deal to facilitate the legal recognition of electronic documents. However, in

Continued on page 27

NETWATCH

By Annabel Lane, Nestle UK Ltd

Welcome to the new year and a new Netwatch. Have you been thinking about IS security and audit over the break? No? Well what about career management? A new year, a new start, that sort of thing?

It seemed an apt time to open with a review of a site that is perhaps slightly outside the usual for this column - the new career management site that Barclay Simpson have set up.

www.barclaysimpson.com

After the Christmas break, perhaps some of us have been spending our time contemplating our lives and may even have decided to consider a move for the New Year. If you are considering this, or even just want to keep up with the market trends, then this site is worth a look. There are quite a lot of sites out there in the recruitment arena, but Barclay Simpson, as you know as a regular reader of this magazine, specialise in vacancies in internal audit, including computer audit, and their site claims to provide the largest database of live permanent and temporary vacancies in the industry.

On first entry you are offered a range of options. Under current vacancies you can register for email updates or have a look at vacancies which are grouped by industry and type of vacancy, e.g. Banking and Finance, Computer audit and security. When I had a look there were some interesting opportunities listed - but don't tell my boss I said that!!

But of course, not everyone logging on to this site will be looking to change jobs. A great many of us will just be after information on matters of interest and advice. There is plenty of that too. There's a bulletin which is regularly updated on the state of the recruitment market and the types of salary level changes that internal auditors moving jobs can achieve. If you were thinking of changing industry, or were just interested in how audit tends to operate on a general level in other sectors, there is a section which explores career opportunities in particular sectors, such as banking, manufacturing, etc. Within these are client profiles in which large companies within those sectors describe their operations and set out how they go about audit. I thought that was particularly interesting.

Interested in Turnbull and how it will affect you and audit/risk management? It gets a separate section here. Or you can order Barclay Simpson's free publications such as "An Introduction to Computer Audit" with a click of the mouse. (Okay a few more clicks than that!)

I think the career management section is also very interesting. It covers topics such as where to live and work in the UK for audit jobs and you can use it to link in to geographical areas in which you might be interested. Also there's a lengthy article on the professional qualifications that might be considered by auditors - of course CISA is included and there's a link to the ISACA web site.

If you are inclined to register you can have vacancies sent to you and gain access to the open forum. When I checked it out there were no discussion threads in progress…an opportunity for us to start some perhaps!

www.silicon.com

There's a lot of information on ebusiness available out there and this site is no exception. Mainly dedicated to news items and the stock market it has the type of news archive you'd expect with security blunders and virus break outs listed. There is also comment - when I visited there were some "behind the headlines" type analysis of issues like the RIP bill which affects us all. For some high level information check out the "decision makers" zone which deals with issues such as the RIP bill and leadership. Generally a well set out site - but I did find the repetitive music rather irritating after a while!!!

www.eSecurityOnline.com

This is a site which is actually set up by Ernst and Young and supported by them, but this is quite subtly displayed on the home page. It has a wealth of information available to the user.

For example, the home page has a link to a database of news items which purports to contain over 6,000, all on the subject of e-security - hacking, encryption, viruses and so on. There's also a database of tools you can browse if you are looking for something specific like encryption software, plus a list of the latest vulnerabilities that have been notified, events that are coming up and recommended books. Many of these can also be accessed by clicking on the tabs along the top of the page. For example the vulnerabilities page gives you a list of the current "top five" and you can subscribe to the online vulnerability news service which continually updates you from the research carried out by the E&Y team, though this is a chargeable service. Clicking on the virus tab gives access to a searchable database of viruses by name. Very handy for those emails we all get telling us about some new and dreadful virus which does terrible things and we must all tell every one we know about it immediately even though it is a complete hoax, as a database like this soon tells us.

If you like to receive this type of thing directly into your inbox you can sign up for the free newsletter. This lists important news items, and important new vulnerabilities and viruses that have been discovered, regulatory news and guidance on best practice for securing systems, which could be useful in a technical audit of that particular area or system.

A page on the site that I found particularly interesting was that devoted to resources. This contains many other links to sites. For example there is a panel dedicated to organisations which publish security information and news groups on the security subject. There is a list of security qualifications - of course CISA is included with a link through to the main ISACA site, along with others which might be of interest to use such as CISSP. And if you're a real in box aficionado, there are plenty of other mailing lists here to which you can subscribe - clicking on the link takes you through to a huge list of them all and instructions as to how to become a member of the list.

The Archive and Resources area at the bottom of this page claims to list security web sites with unique content. They are dedicated in the main to the work of hackers and one which I thought was quite interesting is reviewed below….

www.attrition.org

Attrition organisation claims to provide space for " a lot of stuff that just doesn't fit anywhere else" and looking at the main page (black background - always a give away!!) there certainly appear to be a wide range of all sorts of subversive subjects covered!

Checking out the security page, it seems to be written from the point of view of exposing flaws and vulnerabilities to assist network administrators in identifying and closing these off - for example the paper on strategic scanning and assessments of remote hosts which goes into a fair bit of detail on this. There are also pages devoted to news and archives dedicated to viruses, cryptography, and so on.

If you're having problems convincing the powers that be of the damage that can be done to your company's reputation by a hack that defaces your web site, you could sign up to attrition's email list which automatically inform you of new

defacements as they happen.

http://www.isaca-london.org

And don't forget to check out our very own site, continually updated by our resident webmaster, Allan. A recent addition to the site is the discussion forum page. This could be a very useful resource for members and some have been using it already. So get out there, get lurking and get posting!!!

I heard about a very nasty virus the other day and thought it was my duty to pass it on to you all as the writer demanded. So here is your warning! (Tongue firmly in cheek!)

If you receive an email entitled "Badtimes" delete it immediately. Do not open it. Apparently this one is pretty nasty. It will not only erase everything on your hard drive, but it will also delete anything on disks within 20 feet of your computer. It demagnetises the stripes on ALL of your credit cards. It reprograms your ATM access code, screws up the tracking on your VCR and uses subspace field harmonics to scratch any CDs you attempt to play. It will program your phone auto dial to call only your mother-in-law's number. This virus will mix antifreeze into your fish tank. It will drink all your beer. (For God's sake, are you LISTENING?!?!) It will leave dirty socks on the coffee table when you are expecting company. It will replace your shampoo with Immac and your Immac with Regaine, all the while dating your current boy/girlfriend behind your back and billing their hotel rendezvous to your Visa card. It will rewrite your backup files, changing all your active verbs to passive tense and incorporating undetectable mis-spellings which grossly change the interpretations of key sentences.

If the "Badtimes" message is opened in a Windows 95/98 environment, it will leave the toilet seat up and leave your hair dryer plugged in dangerously close to a full bathtub.

****WARN AS MANY PEOPLE AS YOU CAN****
Quick! Get busy! Send send send send send.....

INTERNET RESOURCE LIST

AUDIT

http://www.isaca-london.org
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
www.barclaysimpson.com

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
www.eSecurityOnline.com

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

NT's Ultimate Countermeasure - a Strong Password

Karen Nelson, Insight Consulting Limited

As I begin the first of this four part series on Windows NT 4 and 2000 security, Microsoft security has just been breached three times in less than two weeks.

The incident reinforces the contribution that information systems audit can make to the enterprise by continuously reviewing the organisation's ongoing security awareness campaign's, it's methods of monitoring for weaknesses, vulnerabilities, and intrusions; its emergency response and incident handling procedures, and how well its configuration and implementation of technology enforce its security policies and business requirements.

Two features of NT make it particularly vulnerable to attack, according to the book ***"Hacking Exposed"*** its backwards compatibility and ease of use. One of the most easily exploitable features of Windows 2000 is its backwards compatibility with LanManager weak authentication. Since the technology is easy to use, it is often used for rapid deployment with little consideration given for best-practice security configuration.

"The Ultimate CounterMeasure - a Strong Password"

Throughout their book, ***"Hacking Exposed",*** the author's emphasis the importance of using strong passwords. It is relatively easy to find and use password cracking tools, network sniffers and eavesdropping utilities, trojan programs and remote control software, and capture password lists to break accounts with elevated privileges, and then carry out unauthorised activity with a seemingly legitimate account. Therefore, poor enforcement of password policies can place an organisation's security at high risk.

In NT based networks, hackers will target the Administrator's password because it has capabilities that can be used to take control of the system and to launch remote attacks. The primary mechanism for gaining administrative privilege is by guessing passwords. Successfully guessing the password is likely because users tend to choose easy passwords, such as blank passwords, something easy to remember, or they fail to change default passwords of software running under the context of highly privileged NT system or administrative accounts. Crackers who methodically gather information about the network infrastructure will find test machines, shares, or poorly protected servers and power-user workstations to target to gain access and infiltrate the system. [McClure, Scambray and Kurtz describe in detail the techniques and tools employed for gleaning information to use in attacking an organisation.]

The Administrator password, by default, cannot be locked out by unsuccessful logon attempts. However, the Microsoft NT Resource Kit contains a utility, passprop that can be configured to enable account lockout for Administrator. Often weak password policies are chosen for the administrative account. For example, account options often include "the password never expires." The administrator may not have changed the password since initial set up. The administrator may be shared by a group of technical staff. Administrative accounts of consultants who have left the company may remain active.

Standalone servers that are members of the domain, such as Internet Information Server and SQL Server, frequently become the target of attack. Using information obtained from hacking these servers, the hackers may gain escalated privileges required to impersonate domain accounts.

NT can be configured to eliminate many weaknesses and known vulnerabilities that contribute to success of password attacks. Simply installing the latest Service Pack or Hot Fixes does not ensure password protection improvements are implemented. Most of these tools are not automatically installed and must be configured. This article discusses the top 10 techniques for reducing vulnerabilities to password attacks:

1. Verify that security policy and baseline security standards have been adopted and check the configuration against these policies and standards.

2. Check account policies

configured in the NT User Manager that set password expiration, minimum password age, length, history, lockout policies and lockout duration, and implementation of SOPs.

3. Change password filtering and notification.

4. Set strong encryption of the SAM database.

5. Disable LM authentication on Windows NT.

6. Restrict information available to anonymous logon users.

7. Change default passwords of required accounts.

8. Protect the registry from unauthorised disclosure and use.

9. Enable auditing of account/ password changes.

10. Strengthen the network perimeter to prevent eavesdropping and sniffing.

Adopt Policies and Baseline Standards

The best start at protecting the network is to set security policies and baseline standards that are adopted and approved for use by business managers. Password and account policies and baseline standards should be based on the results of risk analysis, legal and regulatory requirements and business objectives. The risk analysis should identify the expected impact to business operations of loss of confidentiality, integrity or availability of information systems. It also should identify the most likely occurring vulnerabilities and threats and probability of occurrence. When technical support staff and end users share a common understanding of management's planned controls over information security, they are more likely to take actions required to protect information system assets. Published (electronic or paper-based) policies and baseline standards, along with periodic security awareness campaigns, make it easier to implement management's intentions in managing security and bolstering strong password controls.

Configure Strong NT Account Policies

The NT 4.0 account policies can be set to allow blank passwords, to prevent password expiration, and to prevent lockout. The policies should be checked periodically to ensure that the configuration meets the baseline requirements. Also the LAN Administrator may circumvent the configured policies when resetting a password on behalf of the user. Using readily available tools to check the user's actual account settings against the requirement or to conduct password attacks (penetration testing) maybe in order.

Enable Strong Passwords

Password guessing is the easiest attack on the network. Microsoft provides a number of resources and tools for implementing strong passwords. PASSPROP is a tool included with the Windows NT 4 Resource Kit (NTRK) that can be used to require mixed case, numbers or symbols and to enable automatic lockout of the Administrator's password. The PASSFILT.DLL can be used to increase password strength by requiring a passwords of at least six characters, and disallowing the use of username or any part of the a full name in the password. On Windows 2000 strong password enforcement can be enabled by opening the Local Computer Policy MMC snap-in and enabling the "Passwords must meet complexity requirements" setting in Computer Configuration\Software Settings\Account Policy\Password Policy.

Encrypt private password information in the SAM database

The SYSKEY.EXE (System Key) hotfix is an optional strong encryption capability that can be used to encrypt the private password information only in the account database. Every system using the strong encryption has a unique account password encryption key. This key is encrypted with a System Key. The strong encryption of account passwords in the SAM portion of the registry and subsequent backup copies of the registry and on system backup tapes provides extra protection. It can be applied on Primary Domain Controllers, Backup Domain Controllers and workstations. The SYSKEY.EXE utility is used to apply strong encryption and once enabled can defeat programs designed to run brute force and dictionary attacks against the SAM database. SYSKEY can thwart attacks from the hacker utility PWDUMP, however, PWDUMP2 may defeat SYSKEY.

While these products were designed for the Windows NT 4.0 Microsoft has announced that password strengthening tools will be included in its latest hot fixes and service packs for Windows 2000. The tools should be used when using NTLM authentication in a mixed Windows 2000 environment. The table at the end of this article lists key Microsoft documentation on how to implement these optional controls.

Disable LANMAN Authentication

By default Windows NT provides backward compatibility to LAN Manager challenge/response in order to permit login from Windows 9x, Windows for Workgroups and older LAN Manager Servers. LM authentication is not as strong as Windows NT authentication so attackers scavenging network traffic will search for and attack the weaker protocol. The Primary Domain Controller or Windows 2000 controller in a mixed environment which maintains user accounts has been configured to provide password hash information in a form that

downlevel clients can accept. This feature can be exploited to put all NTLM account data at risk. Only configuring a feature of NT Service Pack 4 can eliminate this weakness. A LSA registry entry must be added to set the "LMCompatibilityLevel" at a high enough level to prevent the domain controller from accepting LANMan authentication requests.

Restrict Anonymous Connections

Windows NT by default allows anonymous users to connect and enumerate certain resources such as domain user names and share names without supplying credentials. This is the type of information hackers seek in planning attacks on the network. You may have heard of "Red Button" vulnerability, null session connections or anonymous logon users. The functionality is required by certain services such as Windows NT Explorer, User Manager and ACL editor to administer and manage access control across Windows NT domains. Microsoft has released fixes to the problem in Service Pack 3 and beyond, however, simply installing the Service Pack does not implement the fix. You have to add or change two registry settings:

- If your requirements dictate a more secure environment, allow only authenticated users to list account names and shares and exclude anonymous connections add the registry value "RestrictedAnonymous," Data Type: REG_DWORD, Value 1 - to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA hive.

- To restrict anonymous remote registry access, set the "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\SecurePipeServers\winreg entry. Use "winreg\AllowedPaths" to permit authenticated users who are not explicitly granted access to gain access for printers and other system services.

The registry entry, while it prevents many leaks, does not work against a hacking tool, SID2USER, used to exploit the SID (security identifiers) and eventually gain the Administrator's account. The tool is at http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt.

Change Default Passwords of Required Accounts.

Many software packages commonly installed on NT domain or standalone servers often require the implementation of default accounts and passwords, for example Microsoft SQL Server, Exchange, and SMS Servers, ArcServer backup software. Often these accounts get added to the Domain Admin or Administrator's group and may be used to gain escalated privileges and Administrator level access. [Hacking tools such as "GetAdmin" and "Sechole" also exploit weaknesses and add illegitimate accounts to the Domain Admins group in order to garner special privileges.] These passwords should be change to difficult-to-guess passwords and technical support staff should be given appropriate group memberships that would provide traceability and restricted access according to the principal of least privilege.

Protecting the Registry

Most password cracking tools use a captured password file to precompute a password guessing algorithm and compare the results to the hashed version in the SAM database. The SAM is world readable by default but locked by its system components. Since the SAM data can be stored in a file it can be easily captured and used offline to launch an attack without locking accounts. During installation or creation of emergency repair disks a copy of the password database may be placed in the \WINNT\REPAIR or on diskette as SAM._. The L0phtcrack Tool and other network sniffers can be used to capture password hashes sent over a network. BDCs contain read-write versions of the SAM in order to receive replicated versions of the PDC SAM and frequently become the target of attacks.

Restrict the use of the NT Registry Editor program files to those who business responsibilities require it. Remove "Full Control Everybody" from the SAM portion of the HARWARE_LOCAL Machine. Create entries in HKEY_LOCAL_MACHINE that will limit the groups and users that can connect to the system for remote registry access. Check the "SecurePipeServers," "winreg" and associated subkeys of the "CurrentControlSet". Ensure that registry entries have not be set that enable automatic logon by setting the default username and password.

Enable Auditing of Password

You can enable auditing of failed password attempts in order to detect failed access attempts. Third party utilities are much friendlier than the NT Event viewer for reviewing audit records. Enabling auditing of Server Password and Security registry entries requires the use of special procedures. This requires setting up the Schedule service to open Regedt32 in the system's security context, then adding users such as Domain Admins and Administrators as SAM key users, then select audit permissions on the existing subkeys. Other security relevant events can be auditing by selecting audit parameters for the Security Key as well. Performance Monitor can be configured to track audit events and to send an alert to the administrator based on suspicious activity.

Strengthen the Network Perimeter

Computers connected to the Internet should disable NetBIOS over TCP/IP and the DNS Servers should be configured to prevent disclosure of address records to anonymous users.

Many hacker tools employ NetBIOS scanners to obtain lists of shares, identify machines used as PDCs and BDCs, and to launch eavesdropping attacks, password attacks, and penetration tests.

More information on secure configuration of NT passwords and account is available from Microsoft at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes and http://support.microsoft.com.

The table below lists relevant MS Knowledge Base reference codes.

	Reference Code
Information on Restrict/Anonymous	Q155363
How to Disable LM Authentication on Windows NT	Q147706
How to Password Change Filtering and Notification in Windows NT	Q151082, Q161990
Windows NT System Key Permits Strong Encryption of SAM	Q143475
Restricting Information Available to Anonymous Logon Users	Q143474
How to Enable Automatic Login to Windows (don't do this)	Q97597
Enable Auditing of NT Server Password Registry	Q186374
Restrict Remote Registry Access	Q155363
Administrators Can Display Service Account Passwords	Q184017
Protection of Administrator Account in Offline Windows 2000 SAM	Q223301

MIND GAMES
by Puzz

This puzzle requires dedicated analysis, powers of deduction and sheer slog to resolve.
(With thanks to Reader's Digest for the basic format !)

1. **There are five companies in a row on the Bloggs Industrial Estate, each with a different coloured logo, and run by directors of different nationalities. Each man has a different make of company car, has his own particular favourite daytime drink, and each has a different pet.**
2. **The Englishman runs the company with the red logo.**
3. **The Spaniard owns the dog.**
4. **Coffee is drunk by the man who owns the company with the green logo.**
5. **The Ukranian drinks tea.**
6. **The company with the green logo is immediately to the right (your right) of the company with the white logo.**
7. **The Mercedes driver has pet snails.**
8. **The Ferrari is driven by the owner of the company with the yellow logo.**
9. **Milk is drunk in the middle company.**
10. **The Norwegian owns the first company (on the left).**
11. **The man who drives the BMW runs the company next to the man with the pet fox.**
12. **The Ferrari driver runs the company next to the company whose owner has a horse.**
13. **The Rolls Royce owner drinks orange juice.**
14. **The Japanese owner drives a Toyota.**
15. **The Norwegian runs the company next door to the company with the blue logo.**

Who drinks water ? ….and, who has a pet zebra ? **Answers on page 28.**

Telephony Security - Phone Tapping

By Duncan McKerracher

In previous editions of Datawatch we outlined three of the four main issues of telephony security namely Toll Fraud, Denial of Service and Corporate Embarrassment. This article describes the fourth and final issue, that of Phone Tapping.

Phone Tapping is regarded as the traditional type of telephone hacking. This involves attaching a "listening device" to the wiring infrastructure to allow the content of a telephone conversation to be heard by an unauthorised person. Such devices can then record conversations that can be later retrieved, or transmitted to a receiver outside your offices. Most organisations need to make sensitive calls of some nature. Speech over telephone lines is not secure and must always be treated with this thought in mind. There are hackers who are employed by competitors to gain secrets that could enable competitors to gain a major competitive edge.

"Listening devices" can be plugged into to your organisation's telephone infrastructure at all or some of the following points:

- the Main Distribution Frame (MDF) that is normally collocated with the PABX containing connections to all telephones within your office,
- the Building Distribution Points (BDP) that distribute a multicore cables fed from the PABX to individual outlets on the wall that are generally located in risers or corridors,
- cable outlets (i.e. wall sockets) and telephone handsets.

The main defence against phone tapping is to establish good physical security that limits the access for strangers to your offices. Your staff must also be made aware of the risks and be vigilant for the signs of phone tapping. Organisations may wish to carry out regular sweeps of their infrastructure using equipment that detects the presence of illegal transmitting devices. These so-called "Bug Detectors" are battery-operated, hand-held devices that can detect a transmitter over a short range. They are easy-to-use and cost in the region of £1,000. To detect recording devices, a physical inspection of the infrastructure is required.

The protection of information about your telephone network is key to preventing phone tapping. One of the recent trends in telephone hacking is the use of "Dumpster Diving". This involves the sifting of an organisation's rubbish bins in a bid to salvage classified information about the configuration of the telephone system. This includes documents such as:

- Call logging printouts
- PABX and wiring configuration details
- Internal and external correspondence
- Internal telephone directories and user guides

All, or just some of the above documents can provide invaluable information to a hacker in a bid to hack a telephone network. A policy to dispose of classified information should be established and implemented. It is also important that documents such as the internal telephone directory and telephone system user guides do not contain information that could be of use to a hacker.

In addition to protecting the content of telephone calls, it is also important to protect the information about the nature of the calls, e.g. the destination and source. Information held on the call logger could allow an assessment of an organisation's sensitive areas of work. Therefore, the protection of access to the call logger is important. Additionally, Information held in the call logger (such as modem extension numbers) could be used to make qualified judgements about how best to hack the telephone and data network. For these reasons it is important to prevent unauthorised remote access to the call loggers.

In conclusion, Phone Tapping is a real risk to your organisation's security. However, many organisations remain ignorant or unconcerned about this risk. By implementing simple procedures it is possible to minimise the risk of at a comparatively low cost.

Duncan McKerracher BEng is an independent Telecoms Consultant specialising in Fraud and Security issues. He is a member of the Telecommunication 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.

Research

By Kamal Khan

The aim of the IS Audit and Control Foundation (ISACF) is "…to provide meaningful, co-ordinated and proactive research ideas, develop and document those ideas, and to continue to refine the research framework incorporating COBIT, and IT Governance related ideas and projects.".

Some of the benefits to members of this research are:

- as the technological environment changes and evolves, new threats arise; this requires constant research to research the new technology, what threats they represent and ways of controlling them; most publications have control objectives based on COBIT or CONCT as well as an audit program;
- knowledge about relevant subjects is created and shared through ISACA's many channels which include the website, the Control Journal, conferences and seminars;
- as every aspect of our lives is now dependant on Information Technology; it is essential to have a professional approach to managing it, and sound and timely research facilitates this.

Research projects are identified, funding is arranged and managed centrally by the ISACF Research Board through Rolling Meadows. This should ensure that the best use is made of the Association's resources - financial and technical. In addition, the Board is responsible for ensuring that the research is of a high quality and of benefit to its audience.

In identifying relevant research projects the Research Board has to consider as its stakeholders Government, accounting bodies, Commerce and Industry, Finance as well as the general public. Its audience consists of not only IT Auditors, but also risk management professionals, IT consultants, CIO's and IT Performance Auditors.

Specific research projects are identified through proposals received from chapters around the world as well as other membership based organisations with similar interests such as IFAC, AICPA, CICA, IIA and others. Suggestions and recommendations may be received from Foundation Trustees as well as members of the Research Board itself.

There is no readily available source of funding for projects (no part of your membership subs are used for this). However, in the last year for each ISACA member US$25-00 was spent on research. The funds came from:

- donations from Chapters;
- organisations and individuals willing to provide funding;
- volunteers on a complimentary or royalty basis;
- direct funding by organisations;
- partial ('seed') funding by ISACF.

Some of the difficulties involved in developing and conducting a research program and which the Research Board have to address are:

- projects may be identified, approved and researchers available, but not proceed due to a lack of funding;
- there are considerable costs involved in turning a research idea into a useful product - conducting the research itself, as well as production of the final product are expensive;
- there may be legal hurdles concerning intellectual property rights which, while time consuming are eventually resolved;
- while research is a long-term investment, technology does not stand still; what may be today's 'hot' topic may never take off while the converse may also be true; this creates a funding problem because there is a reluctance to commit resources towards a research where the benefits are uncertain;
- the research itself may not meet the needs of the audience as the researchers and authors while experts in their field may not understand the needs of the audience; however, there is a very thorough international review process to avoid this - it can yield as many as 500 recommendations for improvement.

Some of the recently completed projects are:

- Digital Signatures: sponsored by London Chapter and S.W.I.F.T.;
- eCommerce: Global Status report, Enterprise Best Practices and Trading Partner Identification, Registration and Enrolment.

Some of the projects underway are:

- eCommerce: Public Key Infrastructure covering Digital Signatures, Certificates and

The ISACA London Chapter Library Collection

by Bill Hawkins

You may or may not know that the Chapter has a Computer Audit library collection housed at the Guildhall Library in the City of London. John Ivinson initiated the original library collection in 1994 with the purpose of having a 'collection of historic books and journals relating to the development of computing as a profession'.

The Chapter Board, following recent discussion, have decided to revamp the library collection but still continuing on an historical basis. The idea of having a library of current publications was discussed but thought both impractical and potentially expensive.

The Guildhall library is keen to hold the collection as it gives an aspect on the City's institutional business life and the development of computer audit in general. I am informed that the collection, while being relatively small at the moment, is regularly referred to by both academics and the public for research purposes.

To be honest the content of the collection was very much a hotch-potch of books and journals. However, the collection has now been rationalised by one of the senior Guildhall Librarians and both the Board and the Librarian are keen to receive book/publication donations. A recent major donation has just been received from one of the Chapter members, Ian Beale (Nationwide).

So if you have any books ready for disposal, please do not automatically throw them away, contact the librarian to discuss the matter first. The Librarian is Irene Gilchrist (tel: 020 7332 1123, email: irene.gilchrist@corpoflondon.gov.uk) A basic guideline for suitable donations would include, a standard/benchmark type book, specific issue book (e.g. digital signatures), books broadly related to computing within London (e.g. report on the London Ambulance Service), books/publications of national importance (e.g. Year 2000) etc.

The Librarian will be writing a fuller report within the next issue of Datawatch and the Chapters web site will shortly contain further details.

Bill Hawkins (tel: 020 7332 1296, email: bill.hawkins@corpoflondon.gov.uk)

Continued from overleaf

Certification Authorities; Security Practices covering Firewalls and other control measures;

- Virtual Private Networks: sponsored by Chicago Chapter covering risks and controls, implementation and audit;
- Customer Relationship Management: security, integrity and control funded by Unitech;
- Enterprise Resource Packages: security, integrity and control of SAP, Peoplesoft and Oracle;
- Wireless: security and risk management with researchers from Verizon;
- Information Integrity: this will involve carrying out qualitative and quantitative research into risks and techniques for information integrity as well as a framework;
- OS/390: a researcher has been identified in Denmark to cover the Information Security issues of this major upgrade to MVS;
- Oracle: this will be an update of the 1993 monograph, covering the latest release of this DBMS as well as Internet related issues.

Some of the future projects being planned could cover IT Outsourcing, network resource management, information privacy, eBusiness benefit realisation and knowledge management. There may also be research carried out as part of the IT Security Technical Series covering Windows 2000, Linux and single sign-on.

So, how can you help in ISACA keep in the forefront of the IS control field? Some possible ways are:

- you could provide a donation when renewing your membership;
- you could volunteer to do some research on a particular topic - either on a complimentary or royalty basis - the research will have to be scoped and approved by ISACF first;
- you could encourage your organisation to donate to ISACF generally or for a particular project that is relevant to it;
- you should use ISACF publications that are made available through the ISACA Bookstore and Amazon.com.

Kamal Khan is currently a member of ISACF Research Board

The Security Column

By John Hunter

DOT-COM! OK, that's got your attention and made sure that this article is topical. It seems everybody wants to be on the "dot-com" bandwagon, throwing caution and basic security to the wind.

With the New Year here I was reflecting on some of the funny incidents reported last year. One of my favourites comes from 'The New Yorker' which ran a piece called "My Fake Job," in which a writer Rodney Rothman recounted his days of masquerading as an employee at a Manhattan dot-com consultancy.

Apparently he is quoted as saying that he walked into a company's offices and, using a false name, claimed a desk and a telephone extension. He spent three weeks there, enjoying free snacks, company-provided massages and carrying on imaginary business calls from his cubicle.

Of course, you might think that this was a joke as the identity of the company was not revealed. But it didn't take long for some eagle-eyed employees of Internet consultant and Web design company Luminant to recognise the reporter's descriptions of their workplace. (Rothman mentioned in his article that he was provided with a T-shirt printed with "May the e-force be with you.")

Luminant's CEO Jim Corey sent out an e-mail to all employees listing a series of beefed-up security procedures. I copy of this was posted on a public bulletin board. The suggestions included:

"1 Introduce yourself to unfamiliar people. Don't be afraid to ask anyone what they do at Luminant. Hey, it is also a great way to make some friends.

2 Store personal articles such as purses, cell phones, and PDAs out of sight.

3 Make an effort to know what client projects are underway around you and know who is typically involved with these projects.

4 Make sure client information is stored away when you are not using it or when you are gone for the day.

5 Don't allow unfamiliar people to follow you through doors with secure access. While it may seem impolite not to hold the door for someone, you can pardon yourself by saying you will be in trouble if you don't follow company policy and direct them to the proper entrance.

6 Never let anyone, familiar or not, have access to your computer.

7 If you have meetings in the office with non-employees, try to use one of the central conference rooms rather than your individual work area. This can protect you from the potential of exposing confidential client information or our ongoing sales efforts.

8 Make sure that you close locked security doors behind you. Our security doors can't be effective if we leave them propped open."

With all the 'hi-tech' firewalls available, this sounded like good basic advice, though 'stable door' comes to mind. It is scary for a company which boasts on its website that it is one of the MasterCard's major e-commerce advisors:

"Luminant was challenged with laying the foundation for MasterCard to build electronic commerce momentum. The credit card company sought new ways to teach consumers how to shop intelligently on the Web by taking advantage of safe merchant and consumer practices, which would subsequently strengthen the company's merchant and financial institution relationships. "

Recruitment

By Adrian Simpson BSc ACA FIIA

If there is one subject that tends to grab people's attention, it is when salaries are mentioned.

Not unreasonably, many are interested to know what they are worth. There is really very little sense in staying with an employer if, other things being equal (which they rarely are) you can earn more elsewhere.

I recently, however, completed an exercise which looked at the average salary increases achieved by internal and computer auditors who changed their job through Barclay Simpson during 2000. The average increase in base salary was 17.5%. At the same time a representative sample of Chief Internal Auditors were asked by how much they had been able to increase their budget for salaries? This came out at 4.6%. Not bad when average earnings in the economy increased by only 3.5%, but rather modest compared with the average salary increase achieved via the recruitment market.

Now, before you start updating your CVs it is perhaps worth looking at the numbers a little more closely.

First the average 17.5% salary increase achieved through the recruitment market is an average, not a typical increase. For example, five computer auditors change job. Four get no increase whatsoever. The fifth gets 50%. Whilst the average increase is 10%, the typical increase is zero.

Whilst our average was made up of a sufficiently high number of placements not to be materially influenced by one or even a significant number of them, our average contained at least two instances of increases of over 100%. It equally included instances where salary reductions occurred. To explain.

If you are a good young computer auditor living and working in the provinces and are willing and able to join an investment bank in London, then in our experience a 17.5% salary increase is the least you could expect. Once increased housing and commuting costs are taken into account, you would need more than 17.5% just to break even. To go from £20,000 to £40,000 can happen. Equally, if you have been made redundant and were earning £50,000 and the only offer on the table is £45,000 - well, after six months of job searching, £45,000 can start looking pretty good.

"...there is no reason to believe that you will automatically lose out financially by staying with one employer,..."

A further consideration is the increasing value of other benefits such as bonuses, profit share and share options. When people are considering a job offer, they tend to include all of these benefits in their existing package, but exclude whatever benefits another company may be offering. There is some justification in this. Many people give up the likelihood of impending bonuses and salary increases with their existing employer and may have to wait over a year to merit them with their new employer. Some of the increase in basic salary can in many instances be a compensation for this.

Still, the 4.6% increase looks rather modest. If that was the average increase available to computer auditors then rather more of them would be out looking for new positions. Many computer auditors received more than that. The three most significant explanations are first, salary budgets are being shared amongst a smaller number of more experienced higher calibre people. Secondly, computer audit departments often lose their more experienced, higher cost individuals. They are replaced by less experienced cheaper individuals. If computer auditors are progressing up through a department and replacing more expensive members of staff, it is possible to offer significant salary increases without increasing the overall budget for salaries. Finally, Chief Internal Auditors, particularly to retain the services of computer auditors, sometimes use regrading or special allowances that are not always awarded from their budgets.

In my experience there is no reason to believe that you will automatically lose out financially by staying with one employer, particularly a good one who is prepared to pay market rates. Those who move jobs tend to have more rounded experience of different audit environments and practices and in the wider employment market will become more marketable. However, more in depth experience of one company may well enhance prospects for promotion within that company. The trick is to recognise as quickly as possible when your career is no longer going to advance. Too many years of 4% salary increases become quite easy to spot on a CV, and does little to enhance your marketability.

So if 17.5% should be ignored as untypical, what is a typical salary increase for changing job? In my experience, most companies will establish your existing salary package and typically offer approximately 10% more. They want to employ someone who feels motivated and pleased to make the move. However, it is also my experience, that if you are young, bright, ambitious and most importantly cheap, you can expect significantly more. Unfortunately, it is also the case, that should your bloom have faded, then rather less may be on offer.

Central News

By Michael Hughes, President, Central UK Chapter

Well another year ends and another year begins, I trust that you have all settled back into work mode after the excesses of the festive season!!

I am sure that you will agree that the Committee has put together an interesting programme of events for you in forthcoming year. Up to date event information can be found on the Chapter's web site www.isaca.org.uk/central. I would encourage you all to visit the site and please let me have your feedback, on good aspects of the site, areas requiring improvement, or any ideas for future development.

Thank you to all of you who replied to our recent Datawatch survey. The general feeling is that that although you do not read it from cover to cover, you do find Datawatch a useful publication. However, you find that the printed format of Datawatch is outdated and would prefer to see it published on the web site. Your comments have been passed onto the London Chapter, who publish Datawatch.

So we are at the start of a new year, what will be the challenges that the Risk Management professional will be facing this year?

No one can pick up a newspaper or IT trade paper without reading about the information age, eSomething, or the latest security breach.

How secure is the future?

As organisations are now fighting to come to terms with the digital economy, a number of traditional IT practices are in need of revitalisation to meet the demands emerging from this new economy. The quality of information and the effectiveness of information management are becoming key differentiators for commercial advantage.

The Government has also established its own e-agenda placing considerable demands on government bodies/agencies to enable them to communicate with their stakeholder base.

Accurate, accessible and secure information is essential to drive and run a modern business. With this backdrop emerges a new manifestation of an old threat - the security breach either internal or external.

Research by KPMG among large UK companies shows that both Dot.Com and traditional "clicks and mortar" companies are leaving themselves and their customers at risk from hacking and cyber crime.

The overwhelming conclusion of the survey is that the new eRisks are not being managed. The phenomenal growth in the use of the Internet has been accompanied by a step change in information risk, but security has not kept up.

98% of respondents said they currently use the Internet. This compares with 70% in the same survey in 1998 and 35% in 1996. However only one-third were sufficiently advanced to be able to undertake business transactions on line. Yet one in six of these still do not have a formal information security policy.

Almost a third of organisations have no Internet firewall to protect them - which for many leaves a back door to their system open to hackers, through a linked web site for example.

Almost two out of five organisations saying the Internet is critical to the operation of their businesses do not have a recovery plan should their Internet connections break down - many of these are Dot.Com companies.

Although almost half of those companies surveyed use what they consider to be advanced encryption techniques to protect their Internet information, this level of encryption can be easily broken.

Two out of five organisations without encryption allow any sort of information to be sent over the Internet.

Over a third do not have an automatic system to report hacking and other attacks coming through the Internet.

Over a quarter have never tested the security of their internet connections by, for example, "ethical hacking".

Security breaches such as virus attacks, theft of equipment and e-mail intrusion show massive growth over the last two years, but evidence shows that organisations are more willing to prosecute offenders.

The other side of the coin is that there are many organisations with no security reporting systems who are simply unaware they have been broken into and highly confidential information has been stolen; they are victims of traceless crime.

Password security is lax as old fashioned words and numbers systems strive to find a balance between effective security and user convenience. However there are the first signs that leading edge companies are using the 21st century password - biometrics, such as scanning thumbprints (representing 1% of the sample). 14% have little or no password security.

The survey also shows that security is not being taken seriously by senior management. Over a half have no formal board level policy - a clear breach of the Turnbull corporate governance rules on significant risk.

Where security is seen as an exclusively IT issue by general management, there is a danger that IT departments will protect the information they see as important and will be unaware of broader business requirements. They fail to understand the criticality and sensitivity of different types of information in use in the business. An example of this is e-mail which often carries the strategic thinking of the firm.

The survey shows that overall awareness of security issues has fallen over last the two years. Users who could be classed as "very aware" have fallen from 24% of respondents to 15%. This may reflect that people now realise how little they know, demonstrating a key need for education at all levels and formal industry qualifications for information security professionals.

However over the last two years all organisations are getting better at managing traditional IT security areas such as information security policy (especially implementation of British Standard Code of Practice for information security management) physical protection of IT equipment and disaster recovery planning.

E-Business offers tremendous potential and great risks at the same time; there are more situations where information and information systems - the corporate crown jewels - are exposed to theft and attack from anywhere in the world.

The risk profile of e-businesses is considerably different from traditional businesses. The recent spectacular security failures involving high profile organisations have been due to simple errors, hacking and denial of service attacks. These have resulted in reputational and brand damage, theft of assets and loss of customers. Senior management has to take information security more seriously now than ever before.

The traditional role of the Information Security Officer has been to manage the risks associated with information, confidentiality, integrity and availability. Yet this narrow definition tends to concentrate on the bits and bytes - there needs to be a change in approach to make e-business work. The definition of security needs to be expanded. For example, as businesses move towards e-businesses, we need to face the issues of trust.

As we continue to move into the new age it interesting to consider that while the tools of the trade may evolve and change and the velocity of transactions increases, a core premise remains:

"The quality of a management decision is highly reliant on the quality of the available management information/intelligence"

So what should we as Risk or Security Management professionals be doing?

As the business value of information increases, the need for securing corporate information assets also increases. We need to ensure that information security issues and their impact on business operations receive Board recognition and that the Board take appropriate action.

All that is left for me to say is Happy New Year and I hope your organisation does not receive headline recognition such as Powergen, Egg, Mircosoft….the list is endless !

Northern Chapter Events

24 January 2001
COBIT III
Gary Hardy, Arthur Andersen
Leeds

28 February 2001
The Key to Information Security
Peter McCready, MBNA Europe
Chester

28 March 2001
Application Service Provision
Nick Goss, Digica Ltd
Salford

25 April 2001
Auditing ERP Systems
Conference
Leeds

Week Commencing 14 May 2001
Auditing e-Commerce
2 day ISACA Professional Seminar
Salford

27 June 2001
AGM & the Future of Commercial Computing
TBA

Are Your Software and Hardware Assets Being Effectively and Efficiently Managed?

10 Key Questions to Consider

1. **Savings Through Bulk Purchases**
   - ✦ What savings do you achieve through hardware and software bulk purchase agreements?
2. **Automated Procurement Process**
   - ✦ How much time is spent on the procurement process (request, selection, authorisation, chasing suppliers, checking delivery, warehousing and invoice payment) - where is time being saved through automation?
3. **Upload to desktops**
   - ✦ How much time is spent uploading software to users' machines (including checking specifications and registering licences) and what controls are in place?
4. **Licences**
   - ✦ How are licences managed for new or existing software (including annual repayments) and software disposals (including under and over licensing)?
5. **Maintenance costs**
   - ✦ How are service contracts and warranties managed, eg are they terminated if unnecessary and do all servers have/need the same criticality?
6. **Hardware Inventory Optimisation**
   - ✦ Can the hardware inventory provide specification information for upgrades and recycling of PC parts?
7. **Inventory Management**
   - ✦ How much time is spent maintaining your software and hardware inventory and reconciling the software to licences and proof of purchase?
8. **Help Desk Efficiency**
   - ✦ What information is immediately available to the help desk to assist in problem solving and can trend analysis be performed on the calls?
9. **IT support staff efficiency**
   - ✦ Can problems be solved remotely to reduce travel costs and time spent?
10. **Server capacity**
    - ✦ Do you have an early alert system for server capacity and imminent downtime?


.....the world's leading computer audit, control and security conferences.....
2001
global events
North America CACS 2001
Orlando, Florida, USA
29 April – 4 May 2001
International Conference 2001
Paris, France
10–13 June 2001
Network Security Conference
Las Vegas, Nevada, USA
August 2001
Asia Pacific CACS 2001
Tokyo, Japan
September 2001
Oceania CACS 2001
Canberra, ACT
23-26 September 2001
Latin America CACS 2001
Mexico City, Mexico (tentative)
October 2001
IS Audit and Control Training Week
February 2001, Houston, Texas USA
March 2001, Philadelphia, Pennsylvania USA
March 2001, Budapest, Hungary
May 2001, Hong Kong, China
September 2001, Toronto, Canada
October 2001, Chicago, Illinois USA
November 2001, Las Vegas, Nevada USA
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: conference@isaca.org
Web site: www.isaca.org
visit our website for details:
www.isaca.org/conf1.htm

ISACA Becomes Founding Partner in New Global Centre for Internet Security

With experts forecasting the online marketplace to exceed US $6 trillion over the next few years, key global enterprises are joining together to reduce risk and implement wise security measures.

As a long-time leader in information technology governance initiatives, the Information Systems Audit and Control Association (ISACA) has become a founding partner in the Centre for Internet Security, a pioneering not-for-profit organisation that is establishing global standards and accreditation systems to promote security and privacy in Internet-related systems.

Other founding partners are the SANS Institute and the Institute of Internal Auditors. The goal of the Centre for Internet Security is to provide the methods used by international organisations to improve, measure, monitor and compare the security status of Internet-connected systems and appliances. This will enable enterprises to effectively manage the risks related to information security.

The Centre will help organisations around the world "harden" their Internet-connected systems. Reducing the risk of significant disruptions from technical failures or deliberate attacks will help ensure the integrity of the electronic business, government, education and consumer information on which society depends. The Centre also will build on existing high-level policy and process guidance to produce specific operational benchmarks that are explicitly measurable. All benchmarks developed by the Centre will be placed in the public domain.

"The mission of the Centre for Internet Security is closely aligned with ISACA's long-term emphasis on international IT governance, control and assurance," said Paul A. Williams, FCA, MBCS, international president of ISACA and partner, Arthur Andersen Financial Markets Division, London, UK. "Effective IT governance supports business goals, maximises the benefits from business investment in IT and appropriately manages IT-related risks. IT governance also helps organisations meet their critical success factors by effectively deploying secure, reliable information and applied technology."

The initial priorities of the Centre focus on three major tasks. It has compared and reconciled differences among security requirements from sources such as the National Institute of Standards and Technology, Internet Engineering Task Force, Control Objectives for Information and related Technology (COBIT®) and SysTrust, and will publish the results. More than 90 charter members of the Centre are reviewing published work on security-enhancing technical actions for specific operating systems and contributing to final benchmarks reflecting global best practices. These benchmarks will be sent to more than 1,000 organisations to provide input on clustering the actions in each benchmark along a "security ruler." Organisations will use this ruler to implement the technical actions required to establish their chosen level of security.

Although the Centre is not tied into any proprietary product or service, it will work with hardware and software developers, network security vendors and consultants to identify steps they can take to help protect their users, clients and partners from Internet-related security problems. According to Clint Kreitner, president/CEO of the Centre for Internet Security, the organisation is using a participative consensus process whereby the knowledge and experience of its members around the world are being brought to bear on the tasks at hand. Using this approach, Centre members are contributing to the development of security benchmarks based on respected best practices for configuration and operation of systems connected to the Internet. To ensure these benchmarks are practical and capable of being implemented and monitored, the Centre will:

- Test and certify commercially available software tools so organisations can establish and maintain compliance with the benchmarks, thus giving them a means to explicitly measure the security status of their systems
- Provide accreditation guidelines for system administrators and auditors to demonstrate a high level of proficiency in implementing and auditing against the benchmarks
- Maintain a security status comparison database populated with anonymous input from automated tools that will enable organisations to compare the status of their information system security against their industry peers
- Keep the benchmarks updated to reflect new threats.

Individuals and organisations with a substantial interest in workable security-enhancing benchmarks are encouraged to become members of the Centre. For more information, visit www.cisecurity.org. For details on IT governance, visit www.ITgovernance.org.

Continued from page 9

considering the 'admissibility' of electronically held data in court legal recognition is only one of a number of factors to be considered in meeting the evidential standards required in most courts of law.

One of the most critical issues in the admissibility of electronic records as evidence is reliability. When a paper document is executed, it becomes fixed in form and content. Subsequent changes to the document are, to one degree or another, identifiable as a by-product of the media (i.e. erasure, reduction and alteration). Electronic media is not so readily "fixed," and changes can be made that are indistinguishable from the original content. Consequently, to ensure durability and consistency of content, methods of recording and storage must be utilised that meet the rigorous standards properly imposed by evidentiary rules.

To qualify as "records" in the evidentiary sense, electronic data must, at a minimum, be:

- Compliant: information keeping must adhere to local jurisdictional requirements for admissibility as "business records."
- Responsible: In that written policies and procedures for record storage and maintenance are established and maintained.
- Implemented: in that the written policies and procedures are employed at all times.
- Consistent: in that the record-maintenance system assures that records stored and maintained are managed in a uniform fashion to ensure credibility.
- Comprehensive: in that all business records are stored and maintained.
- Identifiable: in that all business records for a discrete transaction are readily identifiable and accessible.
- Complete: in that stored records preserve the content and structure of the business transaction creating them to ensure accuracy and understandability.
- Authorised: in that all maintained records must have been stored under the auspices of an authorised creator.
- Preserved: In that records must be inviolate to preserve their original content. No records may be altered without a concise audit trail that preserves relevant information of the original content.
- Removable: in that records may be removed from storage only with the consent of an authorised entity. All removals must be evidenced by an audit trail that preserves the content of the record being removed.
- Usable: in that the information in the stored records must be accessible for general business purposes, for exportation to reporting functions. Any and all accesses (even simple reading) must create an audit trail.
- Description information: ("metadata") must accompany each record. This meta-data allows for persistent explanation of the record stored in order that the origination, content and context of the record may be ascertained 10 months or 10 years later.

These factors need to be considered by any company embarking upon projects which 'digitise records' and destroy original documentation in the process. The economic benefits of digital storage are obvious and compelling but consideration needs to be given to the extent to which key transactional records may be required in litigation as the courts are likely to require proof of the existence and operation of robust internal controls before digitised records can be considered admissible.

Issues to look for during an Audit

For those of you with a penchant for audit checklists, I've listed below some of the key issues to consider from the legal perspective when reviewing e-commerce developments.

- **Ensure that in the terms and conditions statements for services using new delivery channels, there is clarity as to when the company considers a contract to have been formed.**
- **Ensure that Web site design takes into account any local secondary legislation and regulation which governs the formation and legality of contracts.**
- **If the point at which contract formation occurs is important for the product or service delivered, is the legal position clear (e.g. are service providers used? Does the postal or instantaneous rule apply?)**
- **Ensure that the geographical market for the web site is understood and the design takes into account legislation and regulatory requirements applicable to the countries in which potential customers are resident.**
- **In the case of financial services, ensure that there are appropriate means to stop the registration by foreign nationals for regulated products.**
- **Ensure that web sites incorporate a well-constructed clearly written and visible terms and conditions statement with the appropriate disclaimers.**
- **Ensure that appropriate action is taken to register relevant domain names and trademarks.**
- **Ensure that material for**

which the organisation wishes to enforce copyright is not posted on the Web. If such action is unavoidable ensure that the 'Berne Convention' copyright symbol is clearly visible.

- **Ensure that links to other sites do not breach the principles of 'commercial fair play' or 'reasonable expectation of privacy'.**
- **Be wary of the use of framing technology in links, (where this is unavoidable ensure that advertisements on third party sites remain visible).**
- **Ensure that appropriate authorisation for a link is obtained from any sites which require it.**
- **If links are used, ensure that an appropriate disclaimer is visible disassociating the organisation from the content of third party sites.**
- **Ensure that there are adequate procedures for monitoring for possible infringement of corporate trademark names by third parties due to unauthorised Metatag use.**
- **Ensure that there are adequate procedures in place to prevent the organisation using website metatags that inadvertently infringe third party trademarks.**
- **Ensure that e-commerce project managers and sponsors are aware of the data protection requirements at national level and that any proposals for the transfer of personal data between countries takes into account the need to comply with appropriate regulatory controls.**
- **Ensure that appropriate consideration has been given to the use of 'cookies'. If the use of 'cookies' is essential to the development, that deployment and use does not leave the organisation vulnerable to legal action or reputational damage for breach of privacy**
- **Ensure that all employees are aware of their responsibilities to avoid potentially defamatory comments when communicating using both externally and internally.**
- **Ensure that employees, charged with communicating to customers via e-mail, are aware that e-mail communications may be retained by customers and could be legally admissible as evidence of a contract.**
- **Ensure that staff are aware that the principle of vicarious liability could mean that the organisation is legally responsible for contracts inadvertently entered into by employees using using e-mail and Internet access through a corporate PC.**
- **Ensure that employees are aware that the organisation may be legally liable for any postings they make to bulletin boards.**
- **Ensure that organisational management are aware of the current status of the law regarding the monitoring of employee e-mail communications following the Halford case and the possible implications of Human Rights legislation. If monitoring is taking place, ensure that appropriate action has been taken to formulate a monitoring policy and clearly inform employees that monitoring will occur.**
- **Ensure that management are aware of the evidential standards required for electronically stored data and that controls exist to meet such standards and that such controls are complied with.**

Profile of the Author

Andy has fifteen years of experience in computing, eleven of which have been spent in computer audit. His experience spans Local Government, the Health Service and an international conglomerate in the private sector. For the past six years Andy has worked in the financial services sector and is currently an Assistant IT Audit Manager for an International Bank.

Answers to Mind Games on page 16:

The Norwegian drinks water. The Japanese owns the zebra.

Position 1	Position 2	Position 3	Position 4	Position 5
Yellow logo	Blue logo	Red logo	White logo	Green logo
Norwegian	Ukranian	Englishman	Spaniard	Japanese
Fox	Horse	Snails	Dog	Zebra
Water	Tea	Milk	Orange Juice	Coffee
Ferrari	BMW	Mercedes	Rolls Royce	Toyota