,50, Oct-Dec 2001

DATAWATCH

Information Systems Audit and Control Association

DATAWATCH is published by the ISACA London Chapter. Membership of the chapter entitles one to receive an annual subscription to DATAWATCH.

10 Drayhorse Road
Ramsey, Huntingdon
Cambs PE26 1SD
www.isaca.org.uk
nancy@isaca.org.uk

In this issue:

regulars

ISACA London Chapter Committee 2001/2002

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

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

TREASURER
Archie Watt
BDO Stoy Hayward
0207 893 2671
Archie.Watt@bdo.co.uk

SECRETARY
Joseph Wright
0207 260 +6843
joe-wright@supanet.com

MEMBERSHIP/RESEARCH
Kamal Khan
Rabobank International
020 7809 3935
khank@rabo-bank.com

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

PUBLICATIONS/SIGS
John Hunter
HLB Development Consulting
01635 248944
jhunter@hlbdc.com

PUBLICATIONS/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

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

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

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

INTERNATIONAL
Steve Bailey
Steve Bailey Associates
01480 432602
Spart@compuserve.com

EVENTS
Gideon Pretorius
KPMG
Gideon.Pretorius@kpmg.co.uk

EVENTS
Nick Fellows
The Woolwich
0208 298 5646
Nick.Fellows @barclays.co.uk

GENERAL ASSISTANCE
David Spaven
KPMG
0207 311 5620
David.Spaven@kpmg.co.uk

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
Deloitte & Touche
peter.thompson@deloitte.co.uk

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

CISA CO-ORDINATOR
Gan Subramaniam
Homeloan Management Ltd
01756 692147
gsubramaniam@skipton.co.uk

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

WEBMASTER
Peter McCready
MBNA Europe Bank
01244 67200
www.isaca.org.uk/northern

ISACA Central UK Committee (officers only)

PRESIDENT
Mike Hughes
KPMG
0121 232 3207

VICE PRESIDENT/CISA
Simon Parker
Capital One
0115 843 6456

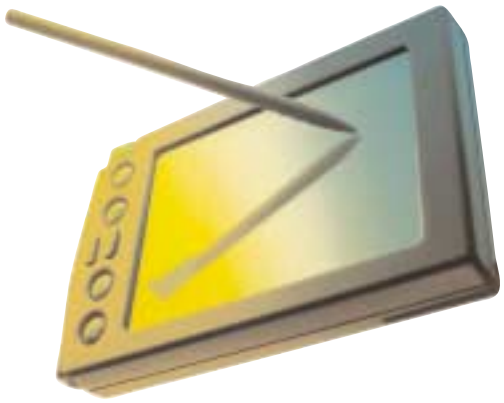
SECRETARY
Chris Chandler
Arthur Andersen
0121 233 2101

TREASURER
Geoff Adey
KPMG
0121 232 3202

PAST PRESIDENT
James Whittaker
BT
0121 230 2214

WEBSITE:

www.isaca.org.uk/central



Hello and welcome to this special edition of Datawatch. As you can see from the cover, it is the 50th ever edition. I wonder how many of you can remember Edition number 1, which would have been back in 1987?

I can't. I'd like to be able to say I was still at primary school then, but an inability to lie forbids that. I certainly hadn't seen the light and started a career in computer audit

Back in those days the chapter was smaller and resources were correspondingly less. Those editors did a sterling job in putting together a newsletter, often virtually unaided. Datawatch started out as a couple of sheets of paper and grew from there to the award winning magazine quality publication it is now. Progress in technology and sterling efforts from the team have increased its size and quality and there's a substantial amount of work now in putting it together - particularly from Nancy, our Chapter Administrator, who does the fiddly and time consuming work of layout and liasing with the printers.

In this issue we have some technical articles such as a Back to Basics piece from Ray Butler, the second half of Andy Farrington's detailed article on RIPA and a feature on managing the modem threat from Mark White of Xinetica. We also have an article that focuses on 50 editions of and Derek Oliver - insights into the progress of ISACA and the computer audit profession over the years for those of us who are relative newcomers. And Lynn Lawton the International Vice President explains what they are doing with our subscription fees over in the USA.

If anyone is interested in seeing the evolution of Datawatch I understand that there are a great many back numbers held in the Chapter Library at the Guildhall! Meantime, here's to the next 50 editions!

ISACA London Chapter Programme of Events 2001/2002

Thursday 27 September 2001
Security Policy
Brian Shorten, CISA
WorldCom International

Thursday 25 October 2001
Third/Party Vendor Outsourcing
Karen Sharpe, CISA
Deloitte & Touche

Thursday 22 November 2001
Selling Your Recommendations
Lindsay Mercer
BAA

Thursday 13 December 2001
E-Fraud
Ian Henderson
Haymarket Management Services Ltd

Thursday 24 January 2002
E-Systems Commissioning
Gideon Pretorius, CISA
KPMG

Thursday 28 February 2002
E-CAATS
Simon Moore, CISA
BDO Stoy Hayward

Thursday 21 March 2002
Project Audit
Dr John Mitchell, CISA
LHS Business Control

Thursday 25 April 2002
COBIT as an Audit Planning Tool
Charles Mansour, CISA
Woolwich plc

Thursday 23 May 2002
AGM/Firewalls & MIddleware
Jag Kanani
Deloitte & Touche

Thursday 27 June 2002
Desktop Audit
Steve Bailey
Steve Bailey Associates

All meetings will take place at the offices of ABN AMRO commencing at 5.00pm

MIND GAMES by Puzz

How many words of three letters or more can you find from the word

E-COMMERCE

15 words: good
20 words: very good
25 words or more : excellent
Answers on page 28

From The President

I, like many others, feel very subdued and concerned as I sit here writing this column in the wake of the New York terrorist attacks. Along with many other Chapter Presidents from all over the world, I sent a message of sympathy from the London Chapter to our ISACA colleagues in New York and Washington, but words just aren't enough.

Many think that the world will never be the same again and, so far, reports of cutbacks in the airline industry preceding what may well be a severe world economic recession and, quite unthinkably only a short time ago, preparations for war, would seem to support that view. All that most of us can do is take a deep breath and hope that things are not going to be as bad as we fear.

Talk about the economy and business somehow felt inappropriate in the immediate aftermath of the attacks. However, as the markets in New York try to achieve some semblance of normality, the press is increasingly turning its attention to disaster recovery issues. Of course, there has been severe disruption to business, but the fact that the markets and so many businesses were up and running so quickly is indicative of the success of their business continuity and disaster recovery plans. It has to be said that the companies worst affected on this occasion are from the financial services sector that is most likely to be prepared. The story might have been quite different if they were from other sectors.

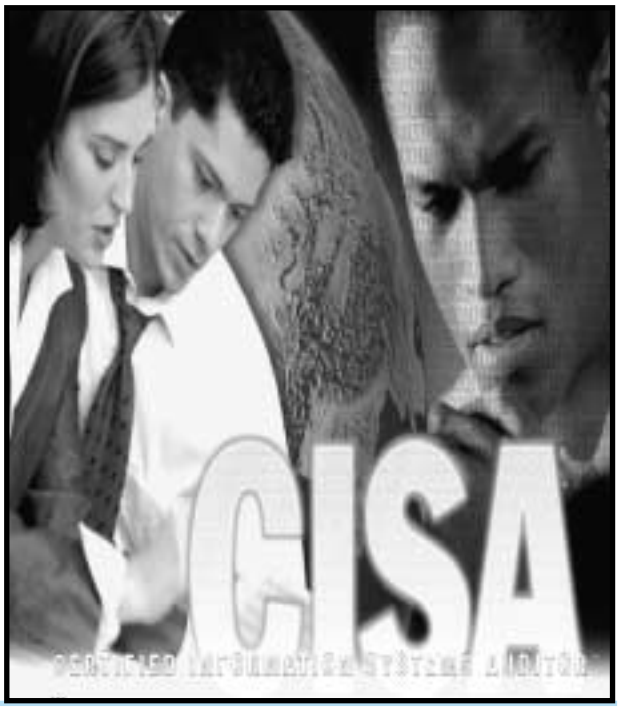
How well would our own companies have fared? It is reasonable to assume that many would not have achieved the level of success that seems to have been experienced in New York. The Gartner Group reports that 40% of companies do not survive a disaster to their computer systems and data. Ensuring that our companies are one of the more fortunate 60% that do survive is something that we should be taking a lead on. That said however, one thing that has been brought into sharp relief is that in the event of a real catastrophe, the first resource that our plans need to deal with and help is our people. Staff grieving for their colleagues or concerned about their families may need counselling or assistance and this is something that we should be factoring in to our plans. After all, at the end of the day, in most companies the most valuable resource goes home at the end of each day.

Moving on from recent tragic events, London has put in another fine performance in the CISA exam this year and I would like to congratulate those of our members who passed. Plans are in hand for the CISA exam in 2002 and anyone interested should, in the first instance, visit our website. If you need further information, please contact Michael Christodoulides, who is always willing to help. In addition, if any trainers out there are interested in providing our CISA review workshop please respond to the invitation to tender, which is included in this DataWatch. Our candidates value this workshop as an important part of their preparation and we always receive positive feedback from them, so do consider getting involved.

All that remains is for me to remind you that ISACA is focussed on helping you to be leaders in the field of information systems audit and security. There are many resources available to you already, such as our knowledge database, K-Net, but if there is anything missing from your skills toolkit that you think we should be helping you with, just let me or any of the Board Members know.

Until next time, keep safe.

Karen



The world's leading conference for IS audit, control and security

north america cacs

North America CACS

5-10 May 2002

Fairmont Hotel

San Francisco, CA USA

For Conference Information:

Visit our web site: www.isaca.org/nacacs2002.htm

Earn up to 44 CPE Hours

North America CACS is presented by Information Systems Audit and Control Association®

Scal-ficate

Managing the Modem Threat

"...most large companies are [probably] more vulnerable through poorly inventoried modem lines than via firewall-protected Internet gateways"
Hacking Exposed: Network Security Secrets and Solutions (2nd edition). McClure, Scambray & Kurtz. Osborne, 2001

"Unauthorised modems are one of the most overlooked security flaws in corporations today. Companies often have modem lines they don't even know are there."
Information Week

Hardly a week goes by where the news isn't full of the latest defacement of a website, or accidental disclosure or theft of credit card details or personal information. It's the Internet which attracts media attention when there is a security breach, which is hardly surprising given that that is how most organisations present their public face to the world. However, as the two quotations above reveal, there is a far more pervasive and insidious threat presented by the humble modem. In this paper we'll explain why this is the case and what can be done to both quantify and minimise the risks.

History of Modem Use

Within any medium to large organisation, our experience tells us that it is very rare for modem use not to be widespread, for a variety of reasons. Historically, since modems came into mainstream use in the early 1980s, it was the modem that provided data connectivity for and between businesses. The whole point of a modem was to allow a digital connection to be made across an analogue telephone system, often to allow remote support of a company's computer system(s), or else to allow the timely transmission of data between two disconnected sites. Even into the early 1990's modems were generally expensive, and (from personal experience) required some skill to install and configure correctly. For business use, hardware cost is generally less of an issue, where it can be balanced against the savings in support costs, and increased efficiency. As business use of computers increased, so did modem use. Modems started to provide electronic links between businesses to provide functions such as EDI and financial transfers (the embryonic business-to-business transactions), as well as fulfilling their traditional support role.

As the pace of electronic change increased, business use of modems also increased. Businesses used more complex computer systems, and automated more tasks. Data became a key asset. Availability of data, and hence computer systems became a business driver. As a consequence, the timely support of a system also became critical. Often the only way of guaranteeing the required level of support from a vendor was by allowing them to have dial-in access to the systems that they were contracted to support. Furthermore, as more and more equipment manufacturers have availed themselves of mainstream computer technology, the inclusion of a modem meant that they could streamline and rationalise their support, to the extent that this is now likely to encompass your telephone systems, fault tolerant disk arrays and key elements of network infrastructure (such as hubs and routers).

In comparison to this long history of modem connectivity, Internet penetration into business processes is a relatively new phenomenon. Even in the US, this year will see only 40% of medium to large companies conduct e-commerce through the Internet, though 98% have an Internet presence. Undoubtedly, given both the numbers of computerised systems that use modems, and the reliance on older legacy systems to conduct traditional business-to-business transactions, it is hard to imagine how modem usage within large businesses could not be ubiquitous.

The Risk to Business

So, given that we have been living with widespread modem usage for almost two decades,

what has changed to increase the risk to business? Undoubtedly there have always been dedicated hackers who have exploited unsecured modems. In the past, before Internet connectivity was prevalent, their primary motivation was more to avail themselves of 'free' telephone calls as a means of accessing bulletin boards in foreign countries. Nowadays, there are two factors affecting risk that need to be taken into account. First, modems are far more widely used in far more business-critical systems than ever before. Consequently, there are more potential targets. The second contributing factor in increasing the risk can be attributed to the PC revolution, which has increased the size of the threat.

Looking back only 5 years, there have been radical changes in the personal computer market, as the table below illustrates. (All figures taken, sadly, from personal experience.)

Table 1.

Description	Typical Cost (1996)	Typical Cost (2001)	Reduction
Entry level PC	£1500	£450	70%
Colour notebook	£2000	£800	60%
Memory (per MB)	£12	£0.12	99%
Disk (per MB)	£0.10	£0.002	98%
Modem	£120	£20	83%

The impact this has had on business is to make computers as ubiquitous a tool as the telephone. It has also added to the burden of modem proliferation, since modems have increasingly become built-ins rather than add-ons (at least within the notebook market). The very fact that computers are in more widespread usage, both at work and in the home, has also led to the rise of the knowledgeable user: users with both the skill and desire to modify and configure their own machines at work.

At the same time there has been an accelerating use of the Internet by home users. In the time that it took home PC usage to increase from just under 40% of UK households to 50% (Jan 1999 - May 2001), home Internet usage increased from 12% to 40. Much of this growth has been stimulated by the introduction of free Internet Service Provision, and the reduction in call charges. (See table below as an example)

Table 2.

ISP	Annual Fee	Formed	Sold	User Base at Sale
Demon	£141	1992	05/98	180,000 (in 8 years)
Freeserve	Free	09/98	07/99	1,500,000 (in 6 mths)

This has a number of indirect impacts on business. First it means that more of their employees are computer literate and Internet aware. The result is more demand for Internet access from work, and more skill in configuring hardware and software (based on experience they have gained at home). The second point is that of the 10 million households that are connected to the Internet, 8 million still connect via modem dial-up.

So, to summarise, businesses have more modem access into and out-of their organisations than ever before:

- more critical systems are supported via modems through dial-in links.
- more employees inside the network perimeter have access to systems with built-in modems (e.g. notebook computers)
- more employees are computer-literate, own modems, and through experience gained at home, have the necessary skills to configure them to access the Internet

Even though, in this paper, we are treating modem-related risks separately from Internet risk, the two are, paradoxically, very closely linked. Employees are motivated to access the Internet from work: it's an entertaining diversion, and saves them money at home. Similarly, the proliferation of home Internet connectivity has equipped 8 million UK households with the tools to breach your perimeter security through your dial-in connections (at a time when, more than ever, hacking is viewed as a 'cool' activity).

Categorising Modem Access

From the above, we have touched on the fact that there are really two distinct aspects to modem access. Dial-out access (where a user internal to your premises uses a modem to access an external system) and dial-in access (where someone external to your premises uses a modem to directly access an internal system). Each poses its own risks, and its own management issues.

Dial-out Access

For most organisations, the risks from dial-out access come primarily from employees subverting the firewall to access blocked content on the Internet. The risks associated with this type of access are twofold:

- Unregulated access to the Internet re-exposes your organisation to precisely the risks that the firewall was designed to keep out. The result is that your systems can be exposed to viruses and trojan horse programs. Equally, an unauthorised connection can be used to download illicit or illegal material (pornography, but also copyrighted works) for which you are then legally responsible.

- All kinds of information can leak out about your organisation: user names, company and machine identification, protocols and programs that you use. All of which can be used indirectly as valuable intelligence by a potential hacker. (See http://grc.com.)

Dial-in Access

One of the common misconceptions is that there is a lower threat from dial-in access because of cost. Why would a hacker bother to dial thousands of numbers within an organisation when it would incur hundreds of pounds in telephone costs? The answer is: because it doesn't. Dialling most organisations at night, only a very small percentage of numbers will be answered. Many of the numbers that do answer are precisely the ones that a hacker would be interested in: modems configured for dial-in access.

Dial-in access poses all of the risks of dial-out access, but with some additional twists.

- As we've covered earlier, your business-critical systems are likely to permit remote access, either as a contractual condition of support, or else as the result of an ad-hoc installation by support staff. So, if someone manages to exploit a dial-in modem, there is an increased chance that it will be attached to a business-critical system.
- A modem which has been added unofficially is far less likely to have been configured securely.
- The attack is more likely to be planned rather than opportunistic: someone is deliberating probing one of your systems, rather than a user stumbling across a site with malicious content.
- It is easy for a hacker to explicitly target your organisation. All they need is a telephone number to start from and then they can dial sequentially.
- A hacker is more likely to have time to exploit the system.
- An attack is likely to be untraceable. Organisations do not usually monitor incoming calls, and there is little on the attacked system to be of use forensically to allow a determination of where an attack came from.

As a result of all of the above, it would be our view that an attack from a disgruntled employee is far more likely to be through an unsecured dial-in connection than through an Internet connection. (They may have even installed the modem in the first place.)

Managing the Problem

One of the initial stumbling blocks to effectively managing modem access can be the attitude of Management itself. Some of the common statements we have come across are listed below.

Once you have overcome the hurdles of the perception of lack of risk, it is important to realise the limitations of what can be achieved practically. For almost any business, modem access in some form is essential. There is little point in trying to impose a no modem policy on a supplier if that is the only

Attitude	Statement	Analysis
Ignorance	"We already have a firewall"	• Modems subvert the firewall (and hence jeopardise the considerable investment)
	"We have a digital telephone exchange"	• Devices are available to allow digital ports to be used by analogue devices (e.g. modems) • Any faxes will use analogue ports.
Complacency	"We know where each modem is"	• How? • What about embedded modems? • Unlikely for any but the smallest organisations, or those with an existing proactive agenda to manage modems.
	"We have a no-modem policy"	• Is the policy effectively communicated? • How is the policy enforced?
Blind Faith	"We know we have a problem - we have other priorities"	• Is this the result of an objective assessment of the relative risks against current priorities?
	"We only have one or two..."	• Is this an assumption or based on knowledge? • That's all it takes!

way that they can achieve a contracted level of service. The key point is to understand the level of modem access that is genuinely required, and remove access where there is no corresponding business justification.

To achieve this goal, we recommend an approach that includes the following steps.

- audit
- assessment
- control
- policy definition
- education

The sequence of the individual steps will very much depend upon an organisation's existing culture, and hence the position from where they start. (The ordering of steps above are suitable for an organisation that does not have an existing modem security policy, for example.)

Audit

The purpose of the audit is to create a baseline understanding of the problem.

- Identify where modems are through:
- Existing telephone lists
- Visual search
- Automated approach
- dentify access controls on a per modem basis
- Iterate through the process - several audits may be required to reveal the full picture (to cover daytime and nighttime usage patterns, for example)

Tools (specifically telephone system scanners, such as our own Xiscan product) can be of real assistance in the audit process, in that they allow repeated scanning of large volumes of telephone numbers. However, whereas they are ideally suited to detecting dial-in access, they cannot accurately reflect the level of dial-out access.

Assessment

Assessment is dependent on the audit results:

- Consider each modem in turn in terms of:
- Function/Usage
- Business Area
- Build business cases for required modems

Control

Take control of modem access:

- Remove unwanted modems
- Ensure modems are correctly configured
- Ensure adequate security controls are in place
- Use good password security
- Remove identifiable banners from internal systems where possible
- Use callback to block access from arbitrary numbers
- Use Authentication mechanisms (e.g. challenge/response, token-based)
- Consider the suitability Integrated dial-up solution as a means to focus control

Control is often a difficult step to implement, particularly where it extends to controlling access of third party suppliers. Password security should ideally reside internally, but be aware of the needs of suppliers to provide support within contracted timescales

Policy Definition

Policy is an important cornerstone. Ideally the policy should not permit any form of unauthorised access, and should aim to reduce the risk presented by modem access. It should:

- Define a strategy that is correct for the organisation
- Document:
- Objectives
- Acceptable use
- Implications for violation
- Create an 'acceptable' modem register

Education

Effective communication of policy is one of the most difficult and often overlooked aspects of the process. It should reinforce both acceptable use and implications of policy violation

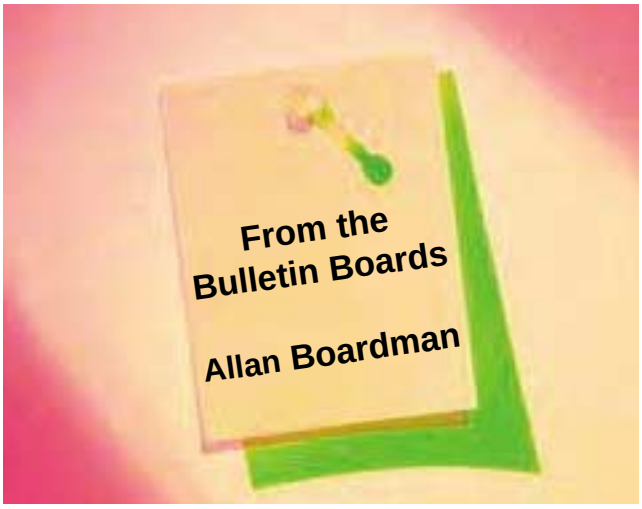
One of the dangers implicit in the ad hoc use of modems is that users are ignorant of the wider implications of such an apparently trivial act. The aim of education is not just to communicate policy but also to raise awareness to the dangers, and thereby get user buy-in. Effective education (backed by policy) is the best tool to address dial-out access. (In this respect, our own Xiscan product is unique in that it can provide automated assistance for education, as well as being used in policing of policy. See www.xiscan.com for the technical details.)

Be Prepared for the Size of the Task

Auditing a telephone network is not a trivial task. The telephony infrastructure must be understood, and any potential impact on normal business processes planned for and contained. Once past the planning stage, there are tools that can help with the job. Telephone system scanners, for example, can provide a great deal of assistance in the audit process, and contribute to education and control.

Continued on page 11...

Another collection of examples from online resources for addressing your pressing information security and audit related issues.



Question:
(http://www.itsecurity.com/asktecs/jul1601.htm)

How detailed should procedures be documented for firewall change control and maintenance? We are auditing the firewall and I'm wondering how detailed the procedures should be for, let's say, opening one port for a needed service. Should there be formal testing? Should there be sign off? If a patch is installed, should there be a documented procedure on what to test - or should the firewall engineers use their knowledge and expertise to figure out what to test depending on what the patch is doing?

Response from Sarah Carter, Director, HarrierZeuros Ltd

Fully documented, accountable and reversible change control is vitally important in any environment. Generally there should be strict guidelines for change, but this depends largely on the organisation, time, cost, benefits, and existing procedure etc.

1. A procedure should be in place for raising a change request - i.e. why does your/the 'business' need the change, what impacts would NOT making the change have, and what benefits would making the change bring?
2. There needs to be a process for ensuring that the requested change is approved by an officer of the company who is responsible for 'information security' (a security manager) - they need to give their reasons for rejecting/approving the request.
3. There needs to be a process for technical approval of the change to assess if it is technically possible. The process should also assess what changes to the firewall will need to be completed and if will it be necessary to try out the changes in a test environment first, or is it safe to carry out the work immediately in the production environment?
4. The change needs to be agreed in terms of a window of opportunity if downtime is needed, or if it can be done during normal business hours then it can be scheduled as part of routine work or a project.
5. All of the processes within this procedure need to be documented (maybe on the intranet, a notebook, or in a workflow software or helpdesk package). This will allow each process to be revisited in the future to review the details of the original request, the authorisation received and changes made so that, should any query/problem occur it can be resolved quickly and easily.

Question:
(http://www.itsecurity.com/asktecs/aug4101.htm)

Can you give me some help on a policy for acceptable use of PDAs in a corporate environment? What technical solutions are available to secure their use and what are the data protection implications?

Response from Amanda Cape, Deloitte & Touche

This is something which we have recently undertaken. As we do not supply PDA's to employees, we were restricted to what we could enforce. However, our policy included: users should ensure that appropriate measures are taken to ensure that any information belonging to the Firm, in particular client sensitive and proprietary information, is suitably protected from accidental loss, destruction or damage.

Therefore, it is the users responsibility to ensure that such devices are handled in a suitable manner reducing the risk of loss or theft. We have obligations to comply with the Data Protection Act. Any PDA, which has downloaded personal data held by the Firm is subject to this Act. The loss, destruction or damage of such data could have serious implications on the Firm. All employees should delete any information, including e-mail, once read. Do not keep any unnecessary information on your PDA. Every precaution must be made taken to minimise the risk of introducing a Virus/Trojan to the corporate network via your PDA. The use of virus software is recommended. PDA's are not considered to be secure computing devices. It is recommended that only non-sensitive information is stored on the device and the password protection feature is enabled where appropriate.

There was an excellent article within Computer Weekly - 16 Aug 2001, which describes the Data Protection Act implications.
www.computerweekly.com

Question:
(http://www.itsecurity.com/asktecs/aug2801.htm)

What are 'web bugs'? Should we be worried about them, and if so, what can we do about them?

Response from Kevin Townsend, Editor, ITsecurity.com

A web bug is a device that secretly reports back to a remote website. It is typically a tiny, invisible gif on the remote site, with a pointer to it in an HTML mail.

Thus, if ITsecurity.com were to use HTML mail, I could include within the message body a link based on <img src="http://www.itsecurity.com/locator.gif" width="1" height="1">. If you open this mail in an HTML-ready e-mail client, you would automatically be sent to ITsecurity.com to fetch the GIF. Because of its size, you would probably notice neither its appearance, nor its fetching, but I would have verified your address as a valid address, and would have added it to my growing database of addresses.

This is particularly relevant to MS Outlook, where the likelihood is that merely looking at the mail will activate the bug. There are methods to defeat the web bug, but most security consultants would simply advise against using a mail client that accepts HTML mail. At best, the web bug is an invasion of privacy - it is usually a 'marketing' device. At worst, however, the principle can be more disturbing. Rather than an invisible GIF, it could be an invisible Frame containing a link to a script on a remote site. If successful, it would download my Trojan onto your system.

The solution? Don't use a mail client that allows HTML. If you must use one, see what remedies are available within the client and within the operating system. But in either case, install a personal firewall that can block both incoming and outgoing.

Thanks to www.itsecurity.com for permission to use the material.

Continued from page 9

However, identifying where modem access exists addresses only one half of the problem. The other half is a management issue: physically finding them and negotiating their removal.

How big the problem turns out to be for your organisation will depend on many factors, not least how seriously the threats posed by modem access have been perceived. In our experience, in organisations where modem usage has been openly permitted in the past (and hence where there is no incentive to hide modems) it is not unusual for 5% of all telephone extensions to be documented as modems. This covers everything from the mainframe computer support down to the catering department! Of these, around 30% will be configured to allow dial-in access. Put another way: for every 1000 telephone extensions, 15 may be providing a direct route into your network through a modem.

As with all aspects of security, the process must be iterative. Policy must adapt to changes in technology and business practices. Having the procedures and tools in place allows you to keep pace with these developments, and monitor whether your policy is being effectively communicated and adhered to.

Mark White has 16 years' experience in IT, and is Xinetica's Product Development Director. Established in early 1996, Xinetica provides expert architecture, development and security services to major blue chip organisations. Xiscan is available both as a managed service and a standalone product. For further information see www.xinetica.com and www.xiscan.com.

Tel: 01925-759838 mark.white@xinetica.com

Part III: Investigation of Electronic Data protected by Encryption

This is the most important section of the Act in terms of the impact upon business particularly business in the financial services sector which relies heavily upon encryption technologies.

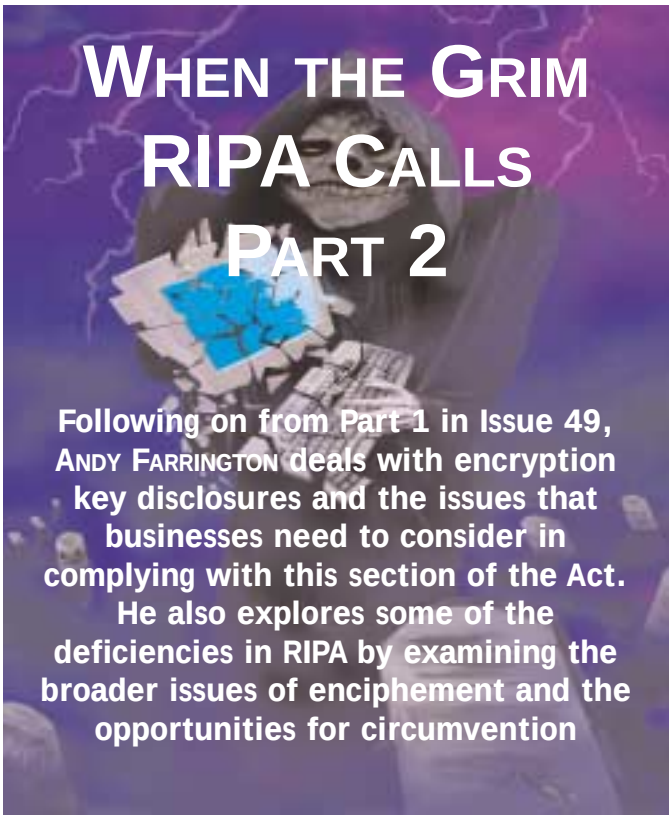
This section of the Act places an obligation on anyone served with an 'appropriate notice' to disclose information protected by encryption in an intelligible form. Under certain circumstances this may require disclosure of the decryption key itself rather than a plain text rendering of the encrypted material. Disclosure is requested by the issue of a 'Section 47 notice' by an 'appropriate public authority'. Warrants can only be issued in respect of encrypted information which has been lawfully obtained.

The Home Office has issued a draft code of practice to aid interpretation of this section of the Act. Examples of circumstances where encrypted information may have been lawfully obtained are listed. These include:

- seizure under a judicial warrant
- disclosure by virtue of a judicial order
- obtained as a result of an interception warrant issued by the Secretary of State under Section 1 of RIPA
- obtained by a Public Authority during the exercise their statutory authority
- has come lawfully into the possession of a public authority
- is likely to come lawfully in the possession of a public authority.

In the case of seizure under a judicial warrant, permission to issue a section 47 decryption notice can be obtained from the same level of authority as the originator of the warrant, e.g. a high Court or Crown Court judge, a Sheriff, a Justice of the Peace, a registered Magistrate in Northern Ireland or any person holding an official position with the same or greater level of authority as a crown Court Judge or Justice of the Peace.

In the case of information obtained via an interception warrant issued by the Secretary of State, a section 47 notice must be authorised by the Secretary of State. The exercise of this option is restricted to the Police, HM Customs and Excise and the persons 'holding office under the Crown'



WHEN THE GRIM RIPA CALLS PART 2

Following on from Part 1 in Issue 49, ANDY FARRINGTON deals with encryption key disclosures and the issues that businesses need to consider in complying with this section of the Act. He also explores some of the deficiencies in RIPA by examining the broader issues of enciphement and the opportunities for circumvention

In circumstances where information is obtained by the Police, HM Customs and Excise, and HM forces through their statutory authority, section 47 notices may be issued by an appropriate level of authority within the department concerned. This means in practice at Superintendent level and above in the Police Force, by the Commissioners of Customs and Excise or an officer they may designate for the purpose, or by someone of Lieutenant Colonel rank or above in the armed forces.

Public authorities seeking a decryption notice for obtained information have to ensure that their application includes all appropriate information. This includes the background to the request, a description of the protected information, confirmation of the manner in which the data has been lawfully obtained, an explanation as to why it is believed that the individual on whom the decryption notice is to be served is in possession of the decryption key, an explanation as to why it is believed that imposing a decryption notice is necessary, a consideration of the proportionality implications of imposing a notice, a consideration as to whether the notice interferes with the personal privacy of the recipient or the owner of the information and, if so, the justification for the interference, a consideration as to why it is not reasonably practicable for the public authority to obtain a plain text of the required information by some other method, and a consideration as to the relative urgency of the application with supporting justification.

The relevant public authority has to retain copies of all applications to serve decryption notices and such permissions must be made available for inspection by a proposed Independent Commissioner with a statutory oversight role.

Section 47 notices must be issued in writing, describe the protected material subject to the notice, contain the office and rank of the individual serving the notice, specify the time period by which the notice is to be complied with and describe what disclosure is required i.e. plain text or the decryption key. The choice of which key to disclose (if there is more than one key which protects the information) rests with the individual receiving the notice. Where permission has been granted for the disclosure to include a secrecy provision, this should be made clear in the notice and

it must be made clear to the recipient that they have the right under section 53(6) of the Act to consult a lawyer on the effect of the notice. Notices will be centrally retained for up to five years after which they cease to have legal effect.

Issues for Business arising from Section III of the Act

1. Verifying the authenticity of notices will be a key issue. 'Notice fraud' could be lucrative for the more sophisticated members of the criminal fraternity. In order to overcome this, the Draft Code of Practice requires that notices contain a unique identifier and the address of an office which the recipient can telephone with the details of the identifier to confirm authenticity. In addition, the person serving the notice must provide identification if asked to do so by the recipient. It is up to business to ensure that anyone that they designate within the organisation as the appropriate point of contact for the receipt of 'section 47' notices is aware of the procedure for verification.

2. The preliminary code of practice states that in the case of businesses, the principles of 'corporate responsibility and administration' must be considered in the issue of notices. This places an obligation on the public authority concerned to establish beforehand, with the organisation concerned, the most appropriate person to receive a decryption notice. This overcomes some earlier criticisms of the process proposed in the original Bill which could have resulted in public authorities serving decryption notices on junior clerical staff. This guidance means that organisations need to consider the level at which a decryption notice should be served. Given that such notices may contain secrecy provisions, the recipient needs to be at a sufficiently high enough level within the organisation to instruct technical staff to arrange for key disclosure or plain text transcription without having to provide a lengthy justification for the request i.e. at senior manager or executive level. There must also be a contingency arrangement in case the senior manager or executive concerned is the subject of a notice.

3. The issuer of the notice must explain to the recipient what is required to be disclosed and by whom, any requirement to disclose a key rather than the plain text, any secrecy provisions, the penalties attached to the notice and how authenticity may be confirmed. Following extensive lobbying during the early stages of the Bill, there is some leeway in the disclosure requirement in relation to "tipping off" (i.e. telling somebody else and running the risk of five years imprisonment) in that it is acknowledged that senior staff may need to consult with technical specialists in order to ensure compliance. There is a requirement for the authority issuing the notice to take reasonable steps to establish in advance who may reasonably be told about the notice in order to ensure compliance. This means that public authorities have to take care that the secrecy provisions are not so draconian as to render compliance impossible for the recipient. These details should be noted on the disclosure notice to avoid any doubt.

4. The modification made to the Bill during its passage through the Lords will come as a relief to many in the Financial Services Industry in that extra tests are required for any public authority demanding a decryption key rather than a plain text decryption of the required information. In such circumstances the requestor has to explain what 'special' circumstances exist in requiring a key and why the object of serving the notice would be defeated if plain text rather than the decryption key itself were to be provided. The main issues here are trust and speed i.e. if the person or organisations subject to the notice are suspected of being involved in criminality and cannot be trusted to provide a bona fide plain text version or if 'timeliness' is an issue and it would take to long to obtain a plain text version then the decryption key may be demanded. Concerns have been expressed that the 'timeliness' provision provides a catch all clause for forcing key disclosure. Assurances have been provided by the Secretary of State that in the case of reputable financial institutions a decryption key will only be required in exceptional circumstances. This has yet to be tested.

5. The Act includes a protection to ensure that a key used only for authentication (e.g. a digital signature) is not disclosed. This raises an important issue for organisations providing certification services under PKI. Organisations will have to ensure that keys used for authentication are distinct from keys used for confidentiality. This will reduce the risk of an authentication key being compromised by disclosure. Given that the recipient has a choice of the key which may be disclosed to render the encrypted message 'intelligible' the disclosure of a session key for decryption will be far less damaging than the disclosure of a private key. This means that organisations will need to ensure internal procedures are established to disclose session keys rather than private keys as this is far less damaging. There may well be implications here in persuading suppliers to amend encryption software to deliver session keys in a timely manner. If an organisation cannot comply within the timescale specified in the notice, and cannot demonstrate that the timescale given in the notice was unreasonable in terms of compliance, the issuing authority has the power to insist on the disclosure of the private key. Another issue concerns the need to ensure that any secret keys used in business activities are assigned as 'company property' to ensure that the highest levels of management have the right to see them, (whether or not they exercise this right is beside the point). This arrangement helps to ensure that notices served at executive level can be more easily complied with as an appropriate 'ownership' arrangement has been established. Companies would also be wise to exercise extreme caution in giving backup keys to trusted third parties.

Continued on page 16...

NETWATCH

ANNABEL LANE takes us on another trawl through cyberspace.
The Internet Resource List is on page 28

I am sure by now you will have noticed that this is the 50th edition of Datawatch (unless of course you eagerly turn to Netwatch first as soon as the magazine lands on your desk or doormat!). It is not, however the 50th Netwatch as when this magazine was founded there were not the resources for audit and security professionals out there in cyberspace that there are now. And let's face it, we probably didn't think of it as there wasn't the material to support a regular column. Any former editors or contributors are most welcome to write in and correct me, of course! Coincidentally, this is my 10th Netwatch column, which though nowhere near the landmark number of 50 is worthy of note, if only for me to marvel how once again I have found yet more sites of interest that I feel I must bring to your attention. The focus this week is once again on security.

www.securityforum.org.uk

This is an interesting site with a lot of information attached. If you register with them (which is free to all till March 2003 if you do it by March 2002) they will send you electronically a kind of newsletter in Adobe acrobat format which I thought was very interesting and well done. There was information such as the latest news on the Code Red worm and articles on email security and the role of the security professional.

At the top of the home page they pick out some links that may be worth visiting for topical reasons - e.g. it is claimed that all you'll ever need to know about Code Red can be found on newsnow.co.uk. Then there are articles on the latest news - a brief thumbnail sketch and the full text is only a click away. This pulls together articles from journals such as Computing and Computerworld. When you click on the article you are also presented with links to a series of connected articles - could be very worthwhile if you are trying to research something particular. Latest events such as conferences also are advertised here - when I looked the subjects ranged from crisis management to CRM. Also highlighted are the latest industry research projects and there is of course a search function too. Very topical, potentially very useful.

http://www.oit.nsw.gov.au/Publications_guidelines.asp#

This is a very different site, run by the Office of Information Technology (OIT) in New South Wales and it contains quite a bit of useful audit information. The OIT's aim is to work closely with businesses in growing the information and communications technology industry in New South Wales. There's plenty of information on why they are there and who's involved. I thought the case studies were quite interesting and would be of use if anything was related to something your company was doing - for example there's one about people accessing their own superannuation accounts over the internet. But what seems to be of most interest to our field is the guidelines section. These amount to guidelines for best practice in areas that many of us are likely to cover in audit or security reviews. For example there are documents on:

- The role of the Chief Information Officer - what his responsibilities should be, who he should report to etc.
- Contracting out of services - rationale, how to tender, how to evaluate, etc.
- Audit of information management
- Risk Management
- Project Management and so on.

Some of the documents have to be downloaded via Acrobat, and others are linked via a mouse click. All in all a useful resource tool for these types of review.

http://webopedia.internet.com/

This comprehensive site describes itself as "the only online dictionary and search engine you need for internet technology". Have a look and see what you

think, but I was quite impressed with it.

The home page is well laid out and lots of information leaps out at you. The search engine is located in the middle and so becomes a prominent feature. You can look at the top 15 terms for which previous visitors have searched and it presents the new additions. When I looked at it, the "headline" article was about the OSI or Open System Interconnection model, which defines a networking framework for implementing protocols in seven layers. It lays out very clearly and succinctly what each of the seven layers does starting from the application layer at the top of the stack, and delving right down to the physical layer at the bottom. Very simply put and demystifying. There's also a diagram showing the layers and how they connect, and within the explanations, clicking on any terms that are underlined takes you to a definition of that term on another page within the site plus further links on this topic that may be of interest.

There are also links to the top technology stories on internet.com if you fancy a browse, and there is a list of subjects down the left hand side of the screen which will take you to lists of other related links and resources. As with many sites these days entering your web address can result in the receipt of a free newsletter. In summary a potentially very useful resource for security professionals.

http://netlingo.com/

Ever feel people are talking in another language? I used to think I was quite familiar with netspeak - words like newbie and flaming, but while my back was turned the world has moved on and I find myself falling increasingly behind the times. That's where sites like this one come in. As its name suggests, it is dedicated to the language of the net. Across the top of the home page, under the banner, are the letters of the alphabet laid out. Clicking on them takes you immediately to the dictionary entries for that letter. E.g. I clicked on D and it presented me with a large list ranging from daemon, DARPA and Data through to dumb terminal, dweeb and dynamic node. Each term is hyper linked so the full definition is merely a mouse click away! It's a more targetted way to access their online dictionary which can be reached by clicking on its title in the contents list. Also in that list is a pocket dictionary which takes the form of a minibrowser or tool bar that you can keep on your desktop for reference if you wish. I thought that was a useful idea. There's also a link to a very comprehensive list of those ubiquitous smileys, more than I ever thought existed. Though I am sure the average person would struggle to use some of them like the "Buck toothed vampire with one tooth missing" and Frank Zappa! (I kid you not!)

Then of course there's a link to all those chat room acronyms - I can't believe that all of these are in regular use either - check them out for yourself and prove me wrong, please! But I am sure that I'll be using some form now on, like "ESO" - Equipment Smarter than Operator! There is a feature on ASCII art (made up with pixels on your screen), international country codes and even an online IQ test which looked a bit hard to me - maybe I should spend more time surfing sites to understand these terms better!

http://hotwired.lycos.com/hardwired/wiredstyle/

A similar site but quite different in feel is this one from lycos. Its home page is quite philosophical and explains how wired style came about - how can we write about machines without losing our sense of poetry? My next audit report is going to be quite different, I can tell you! Clicking on the logo takes you through to a bit more explanation and some further links. I liked "picking nits" which is the editor's pet peeves. The edition I looked at aimed at getting people to differentiate between a domain name and an IP address. There's also "picking brains" which answers a question such as "Where did internet naming convention come from?" and other areas too such as "outtakes and uptakes" which talks about the Outtakes - those items that didn't make it into the pages of the Wired Style book, but work well on the Web, as part of a searchable database. Updates are new items which will appear in Version 2.0 of the book. They can be viewed alphabetically or chronologically (i.e., with the newest entries at the top of the list).

This is an interesting site and aesthetically very pleasing, but for sheer ease of information, you are better off looking at netlingo in my opinion.

Continued from page 13....

A decryption notice can be served on the third party which, under secrecy provisions, would be prevented from communicating receipt of a notice to the organisation which owns the key. Not only would the organisation be unaware that it's encryption keys had been compromised but it would lose any choice in which key to disclose.

6. The disclosure of encryption keys raises particular issues for Banks and other financial institutions who have legal duty of confidentiality. Assurances have been given by the Minister that such institutions will be protected from any breach of confidentiality lawsuits that may arise from compliance with a decryption notice. However there is an obligation to ensure that any breaches to confidentiality are minimised. To this end, the Government has tabled an amendment to the Act, following representations from industry to ensure the establishment of a 'proportionality' test, (Lord Liverpool's amendment). This is designed to take into account the extent and nature of the information protected by the key. There has been a rather belated recognition by the Government that encryption keys in commercial use may protect thousands of individual transactions. The compromise of such a key through disclosure may result in commercial and reputational damage to an organisation which far outweighs the benefits to be obtained by the authorities concerned should the key be disclosed. It may be safer to, post RIPA, to arrange for multiple encryption keys to be used rather than put large numbers of sensitive transactions in one encryption basket.

7. Express consent from the authority responsible for authorising the notice is required before a secrecy clause can be added to the notice i.e. the organisation issuing the notice can not impose a secrecy clause unless this has been expressly agreed and permission granted. A secrecy clause can only be imposed for specific reasons. Firstly, that the required information has come, or is likely to come, into the possession of the UK Customs and Excise, the Police or the Intelligence Services. Secondly, that it is reasonable, in order to maintain the effectiveness of the investigation, or in the interests, safety or well being of any person to keep secret the means by which the information was obtained. The test would be met if it can be demonstrated that there is a specific person from whom it is reasonable to withhold the information. Whether or not the notice includes a secrecy clause, most organisations would not wish the fact they have been served with a notice to become public knowledge. Any organisation that relies upon encryption as a key tool of business, (such as a bank), is unlikely to want the fact that it has been required to hand over a key widely broadcast due to the damage to commercial confidence that may result. This means that organisations need to ensure proper arrangements are put in place to limit the number of staff who are made aware of the event whether or not the notice includes a secrecy requirement.

8. The somewhat draconian measures in the original Bill to deal with 'tipping off' (i.e. up to five years imprisonment, a fine, or both if the recipient of a notice tells anyone about it) have been modified during subsequent readings. There are now statutory defences against accusations of 'tipping off'. Firstly in circumstances where f the software, for security reasons, gives an automatic warning when a key has been disclosed and where it is not reasonable for the recipient to stop this from happening when a disclosure notice is served, the individual may not be subject to prosecution. Secondly, a person receiving a decryption notice with a secrecy clause is permitted to approach a legal professional about the effect of the notice and legal advice may be given. Thirdly, in circumstances where authorised disclosure is made by a lawyer in connection with legal proceedings the individual may not be liable to prosecution.

9. Concerns have been expressed by various commentators about the security of encryption keys once they have been passed onto public authorities. The Draft Code of Practice requires the authority to treat the key obtained under the statutory right to intercept communications as having a Government designation of 'SECRET' together with any material decrypted by using the key. In circumstances where the key is obtained using powers other than the statutory right to intercept communications, the Act requires the authority concerned to exercise the same standard of due care and attention as that given to evidential material destined for use in a court case. This also means that the number of persons to whom the key is disclosed must be kept the minimum commensurate with meeting the requirements of the notice.

10. The Act sets up three commissioners with an oversight responsibility. The Interception of Communications Commissioner will review the permission given by the Secretary of State and the adequacy of the safeguards put in place for the protection of keys. The Commissioner will produce an Annual Report which will be laid before Parliament. The Intelligence Services Commissioner will review the permissions granted by the Secretary of State in respect of the Security and Intelligence Services and evaluate the use made by the Security and Intelligence sources and HM forces of their powers under the Act together with the adequacy of the safeguards put in place by the Intelligence and Security Services and HM Forces for the protection of keys. The Chief Surveillance Commissioner will cover the exercise and performance of any person (other than a judicial authority) in the exercise of Part III powers together with the adequacy of the safeguards for the protection of keys which do not fall within the responsibilities of the other two Commissioners.

11. The Act establishes an Independent Tribunal to whom complaints relating to the exercise of powers in relation to part III of the Act should be addressed. The

tribunal is independent of the Government and has powers to investigate any case that falls within its jurisdiction. In a worrying development in February this year, the Intelligence and Security Committee (2000-2001) Interim Report to Parliament noted that the Tribunal did not have sufficient resources to 'enable it to even open the mail let alone process and investigate complaints'. The fact that the Tribunal is under no obligation to give a right to cross examination, hear oral evidence or to correct inaccuracies in evidence has led several critics to question the fairness of the Tribunal rules.

How effective will RIPA be?

Having spent many hours reading through RIPA and its associated codes of practice, I have concerns about the effectiveness of the Act and perhaps I may be excused if I make some observations about this.. I am not alone in my concerns. In March 2001 the Government's legislative watchdog, the Better Regulation Task Force, recommended that Parts I and III the Act should be examined a year after enactment to determine if they are fulfilling their objectives (the equivalent, in audit terminology, of a post implementation review). This seems eminently sensible and the Home Office, while initially supportive of this proposal, has recently announced that it now sees no benefit in such a review after all. One cannot help but wonder whether there is another agenda at work here.

One may also question the extent to which the Act will protect private citizens against unauthorised interception. The Guardian reported in February a case where text messages and a list of 80 personal numbers were extracted by Ministry of Defence Police from the mislaid mobile telephone of Juliet McBride, a well-known anti-nuclear protestor. Following protests, this case is now subject to a MOD enquiry to determine compliance with RIPA.

It is clear that a key objective of the Act is to overcome the abuse of encryption technologies for criminal purposes and, given the administrative burdens that compliance with the Act may impose upon business, it is reasonable to ask whether the Act is likely to be effective in controlling the criminal exploitation of encryption. This is the crux of the matter. It is clear from the extent of criticism the Act has received from, business, the public, members of the House of Lords as well as academic cryptographers that the Government has displayed a singular lack of understanding of both the technology of encryption and the broader issues associated with encipherment. It would be naive to assume that sophisticated criminals will make the same mistake. It is particularly worrying that an Act, so recently introduced,can be circumvented with such ease. I have detailed below some of the ways in which this could be achieved.

Choosing a small ISP

Most email traffic is routed through a small number of large ISPs. It is these ISPs which are most likely to be targeted by public authorities for interception purposes. and receive interception warrants. It is therefore likely that criminals will migrate from large ISPs to smaller ones to reduce the risks of interception. The cost of enforcing interception warrants on a growing number of small ISPs even on a 'contributory cost' basis will high. Care obviously needs to taken as some smaller ISPs use the services of larger ones. This is perhaps less of an issue if one believes Government assurances that blanket interceptions will not occur. It may be possible to complicate the interception process by using several small ISP accounts and alternating between them to reduce the interception risks even further.

Use an offshore ISP

The risks of interception could be reduced by using email accounts on servers located outside the UK and therefore outside the jurisdiction of RIPA. In such circumstances any email resident on these servers could not be read by the UK authorities without the permission of the relevant jurisdiction. Such services are already offered by 'Safe Web' 'Hush-Mail' and 'MessageRX'. It would appear, in this scenario, that mail could be intercepted when a UK user connects to the overseas hosting service. However, by using Diffie-Hellman key negotiation it is possible to negotiate, generate and use unique keys for mail messages which can then be destroyed when the mail is read. This means that a decryption warrant is ineffective because the keys are ephemeral and cannot be seized. The only place in the UK where the mail could be intercepted would be on the users own computer in the UK and even this may not be possible if the mail is viewed and stored on the remote site and never downloaded. This in turn can be coupled with techniques which allow anonymous access thereby reducing the he risk of allowing the IP address, from which access is requested, being traced.

Use ADSL Technology

ADSL introduces the capability to make a permanent connection to the Internet. With a permanent connection, the need for a mail server is reduced as mail could be routed directly to the PC. This technology is not currently widespread although steady growth is likely to provoke the development of email packages that can utilise direct delivery options rendering interception at the point of the ISP mail server obsolete.

Use Secure Internet Protocols

The Internet protocol Ipv6 which will be introduced in the near future will enable two Internet connected computers to negotiate, use and destroy unique encryption keys used for each data exchange. This mean that keys will be ephemeral and cannot be seized. This protocol is being progressively deployed and will shortly become the standard for all IP data exchange covering email, voice and video.

Use Steganographic Techniques

This is perhaps the most serious countermeasure that could be deployed against RIPA and dramatically demonstrates a fundamental flaw in the Act. Steganography may be defined as 'information hiding'. The success of the interception framework defined under the Act pre-supposes that one is able to identify that a message has actually been sent. With encryption this is comparatively easy as data is scrambled but it's existence is not hidden. With steganography the existence of the message itself is hidden. This would allow messages to be embedded in image files, music files, video clips, even TCP/IP packet headers. This considerably complicates both the interception approach defined within the Act which relies disproportionately on criminals using encrypted email as well as other government interception systems which use dictionary technologies to scan communications traffic for key words or phrases (e.g. the GCHQ/CIA Echalon system and the recently introduced DCS 1000 system deployed by the FBI).

A variation on this is provided by 'Spammimic'. This works by turning any message into a realistic imitation of unsolicited commercial email (euphemistically known as 'spam'). It is a variation on the mimic engines used to turn text into various 'humorous' dialects which are available on a number of websites. From an interception point of view, the message, after translation, cannot be distinguished from genuine unsolicited commercial email - particularly when used with an anonymous remailer. The intention of the author is to develop the engine as a full blown steganographic email system for third party use. If such a system were adopted it would render interception on the basis of keyword searches ineffective. The translation engine is straightforward but this does not matter, as there is no way of distinguishing a message processed through the engine from a 'normal spam'. The intention is not to 'hide the key' as with encryption but to drive up government interception costs to unsustainable levels by forcing interception agencies to process the countless terabytes of unsolicited commercial email that currently clog the arteries of the Internet. A demonstration version of the engine is available on www.spammimic.com, (try it it's a hoot!)

Anderson Needham and Shamir have described a powerful concept known as the 'steganographic file system' in which the filing system of a computer can be set up in such a way that the existence of files can be hidden by a password. This can provide several layers of protection arranged in such a way that disclosure of the top layer provides no information whatsoever about any further layers including their existence. Protection is provided down to byte level on the disk defeating all the commonly used tools for the forensic analysis of computer disks. Systems employing this technique are already available for Linux and Unix operating systems, (StegFs) . The system is incredibly powerful as anyone who gains access to the file systems, even using forensic techniques, can never be sure that they have gained access to all the information that it contains unless they are willing to try all 2^128 possible key combinations.

While working on this article in the summer of 2001 I came across a story, published in an early spring edition of 'USA Today 'which stated that prior to the 1998 American embassy bombings, 'Al Qaeda' - the Bin Laden terrorist network, had been using hidden messages embedded stegonographically in pornographic images on the Internet to communicate between its cells. I have no idea whether this story is true or yet another example of the 'urban myths' that emanate from Internet chat rooms. However, in the original draft I had expressed my concern that such techniques would increasingly be used by well resourced terrorist groups and drug cartels to communicate as they can defeat the traditional methods of interception employed by both the NSA and the FBI. In revisiting this article, after watching, in common with the rest of the world, the horrific events of 11 September unfold on my television screen I can only speculate on whether such techniques were used to help co-ordinate such an atrocity. Perhaps it was not necessary to use such sophisticated methods as there are some indications that the perpetrators used conventional technology with simple open codes to conceal what they were talking about consciously eschewing encryption that would stand out to the security services like a proverbial 'sore thumb'. The use of such a simple technique is both cheap and powerful and without human intelligence even the vast resources of the Echelon network would be unable to distinguish such messages from the petabytes of innocuous data that daily pass through its portals. In such circumstances the very sophistication of the technology and our dependence upon it becomes a weakness that can be exploited.

A more simplistic approach of course would be to use removable media. Authorities seizing the equipment could never be sure that they have acquired all the removable cartridges and as such the capability of authorities to verify what is on the computer is limited by the ingenuity of the criminal in hiding cartridges.

Use covert channels in the TCP/IP protocol

This is a steganographic technique for encoding messages within apparently benign TCP/IP packets. This could defeat conventional email interception and can also be used to surreptitiously tunnel information past packet filters on corporate networks.

The technique exploits the fact that TCP/IP is a connection oriented protocol by encoding information in the TCP/IP header. Typically the header contains both mandatory and optional fields, (the latter of which may be stripped by packet filtering or fragment re-assembly technologies). It is possible to encode ASCII values within the range 0-255 in the IP packet identification field, the TCP initial sequence field and the TCP acknowledged sequence number field. Using this approach, data can be exchanged between hosts while giving the outward appearance of a conventional

'syn-ack' connection sequence. Although somewhat long winded and time consumeing, the technique for doing this is readily available on the Internet. Furthermore the data sent can be encrypted making detection of such techniques particularly difficult. The technique can be incorporated into an O/S kernal or deamon which can automatically send a file whenever a particular site is contacted or whenever the system is in normal operation

It is interesting that communication and exploitation techniques using covert protocol tunneling involving TCP/IP and, the somewhat more useful ICMP protocols are already being discussed on 'hacking' oriented IRC channels.

Specific products designed to defeat RIPA

Most worrying of all, there are a number of new developments underway with the express purpose of defeating both RIPA in the UK, the DCS 1000 system in the US and new laws being introduced by the Australian Parliament. A good example of this is 'M-O-O-T' which is being developed on a non-profit basis by a group of Cryptographers and programmers concerned about civil liberties and on-line privacy.

It is planned to make M-O-O-T available sometime in 2001. The software will consist of a small UNIX based operating system which will be equipped with TCP/IP comms driver and a suite of applications. It will include a layer of unique cryptography which will interface with the application programs and comms using nine discrete algorithms. Because M-O-O-T will disable all local storage completely as part of the start-up sequence, there will be nothing either on the hard drive or removable storage should the computer be seized. Storage will be located in foreign data havens. The encryption algorithms will use Diffe-Hellman ephemeral keys which will be unique to each message so they cannot be seized and because the keys will be padded with random data there will be no way of determining retrospectively what the key was. The messages produced will be hidden steganographically in houskeeping data rendering current interception techniques useless as the existence of a message can neither be detected nor proven. This will permit plausible deniability if a notice is issued requiring plain text decryption of a message, as the issuer will have to prove that the steganographic transcript actually contains a message rather than simply the houskeeping data that it appears to contain. All email addresses and headers will be enciphered defeating traffic analysis. The file system used for storage at the offshore data haven will conform to steganographic techniques. A 'plausible deniability' cipher key will be provided should the authorities require access to the data haven, (which will be a complicated process in some jurisdictions and it is in these jurisdictions that M-O-O-T will seek to locate servers). The deniable key (which will decode certain innocuous information which the user has decided beforehand) can be revealed while ensuring the remainder remains steganographically hidden. No indication will be given of either the existence or nature of further hidden stenographic layers placing the onus open the those issuing a decryption warrant to demonstrate that such layers exist. The operating system and applications will boot from one single multiplatform CD and the intention is to make the CD available as shareware. M-O-O-T will follow an open source development approach to capitalise on the strength of the worldwide cryptographic community to improve the strength, functionality and resilience of the product and ensure that the system remains current in respect to the Law. M-O-O-T is one of several such developments.

In Summary

The Act clearly raises some serious issues which businesses must consider. There are genuine concerns surrounding the introduction of interception technologies into corporate networks. Apart from the cost issues, the technologies could introduce a 'backdoor' for hackers and the risks for businesses associated with a successful 'black box' hack are significant. In addition businesses need to consider the organisation of their cryptographic activities, particularly the nature and range of transactions dependence upon arrangements with third parties and the need to separate authentication from confidentiality. There are also organisational issues to consider such as the corporate ownership of encryption keys, points of contact within the organisation and procedures to authenticate notices while maintaining internal and external confidentiality.

In considering whether the Act is sufficiently robust to provide the security services with a valuable weapon to fight terrorism and drug smuggling I believe that the jury is still out. The sad fact is that the Act in its current form is a flawed artefact which ties itself to particular technologies and appears to concentrate on encryption at the expense of the broader issues of encipherment. It is also worrying that targeting terrorists and drug barons with increasingly sophisticated interception technologies may lead us into a false sense of security, devaluing the powerful human intelligence resources that are an essential part of the equation. Unfortunately I believe that these omissions provide a path around the Act which undesirables will increasingly take using techniques and technologies, which are widely available.

Andy has sixteen years of experience in computing, twelve of which have been spent in computer audit. His experience spans Local Government, the Health Service and an international conglomerate in the private sector. Andy has, for the past seven years, worked in the financial services sector and is currently an IT Audit Manager specialising in E- Commerce for a major International Bank.

All New, Completely Revised CISA® Review Materials

for Exam Preparation and Professional Development

CISA REVIEW MANUAL 2002

Information Systems Audit and Control Association

CISA Review Manual 2002

CODE CRM-2

This manual is updated annually to reflect current industry principles and practices. It provides a comprehensive study guide to assist individuals in preparing for the CISA exam and includes a thorough explanation of the structure and content of the examination, tips on how to develop a study plan, examples of questions and coverage of technical matter outlined in the process and content areas of the exam. This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses.

This manual has been developed and organized to assist in the study of the following process and content areas:

Process Area:
- The IS audit process

Content Areas:
- Management, planning and organization of IS
- Technical infrastructure and operational practices
- Protection of information assets
- Disaster recovery and business Continuity
- Business application system development, acquisition, implementation and maintenance
- Business process evaluation and risk management

The 2002 manual provides definitions and practical examples, as well as references to other helpful study material and a glossary of terms commonly found on the exam. Candidates are urged to determine their own specific strengths and weaknesses as they read through the study material and refer to other sources for additional information where deemed necessary. In addition, review questions are provided at the end of each chapter. These questions are not actual CISA examination questions, but cover similar content and are a source of measuring a candidate's knowledge. Approximately 450 pages. **CRM-2** English Edition (Available October 2001), **CRM-2J** Japanese Edition (Available January 2002), **CRM-2S** Spanish Edition (Available January 2002)

CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS CD-ROM

Information Systems Audit and Control Association

CISA Review Questions, Answers & Explanations CD-ROM, 2002

CODE CDR-2

CISA Review Questions, Answers & Explanations CD-ROM, 2002 consists primarily of the same 600 questions included in the *CISA Review Questions, Answers & Explanations Manual*, 2001 and the 2001 and 2002 Supplements. However, some questions have been removed and others included ensuring proper representation in each content and process area. With this product, CISA candidates can identify strengths and weaknesses by taking random sample exams and breaking the results down by area. Also included are *Information Systems Control Journal* articles referenced in the *2002 CISA Review Manual*. (Available December 2001)

PLEASE NOTE: The CD-ROM requires Windows 3.1 and above and a JavaScript 1.1 enabled browser such as Netscape Communicator 4.05 or Internet Explorer 4.0 (ver 4.72) and above.

2001 CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL

Information Systems Audit and Control Association

CISA Review Questions, Answers & Explanations Manual 2002

CODE QAE-1

This manual consists of the same 400 multiple choice questions published in the *1998 CISA Review Questions, Answers and Explanations Manual* (200 questions), the *1999 Supplement* (100 questions) and *2000 Supplement* (100 questions) formatted in the process and content areas. These questions are selected and provided in two formats.

Questions Sorted by Content Area
Questions, answers and explanations are provided (sorted) by CISA job content area. This allows the CISA candidate to study material by content area and refer to specific questions to evaluate comprehension of the topics covered within each content area. These questions are representative CISA questions, although not actual test items, and are intended to provide the CISA candidate with an understanding of the type and structure of question that has typically appeared on the examination.

Sample Test
These same questions are also provided as a sample test. They have been randomly renumbered to represent a CISA examination. Candidates are urged to use this sample test, and the answer sheet provided, to simulate an actual examination. Many candidates use this exam as a pretest to determine their own specific strengths or weaknesses, or as a final exam. Sample exam answer sheets have been provided for both uses. In addition, a sample exam answer/reference key is included. All sample test questions have been cross-referenced to the 'Questions Sorted by Content Area' so that it is convenient to refer back to the explanations of the correct answers. This publication is ideal to use in conjunction with the *2002 CISA Review Manual*. 166 pages. **QAE-1** (English Edition)

CISA REVIEW QUESTIONS, ANSWERS & EXPLANATIONS MANUAL — 2001 & 2002 SUPPLEMENTS

CISA Review Questions, Answers & Explanations Manual 2001 & 2002

Supplement Codes
QAE-S3 & QAE-S4

Each year ISACA is dedicated to the creation of 100 new sample questions, answers and explanations for candidates to use in preparation for the CISA exam. These items are published as supplements to the *2001 CISA Review Questions, Answers & Explanations Manual* and are ideal for use in conjunction with the *2002 CISA Review Manual*.
(*2001 Supplement*—Available now; 2002 Supplement—Available: November 2001)

www.isaca.org/bookstore

The Career Column

Adrian Simpson

Datawatch issue number 50, DW50 to those in the know, may one day be looked upon as a landmark in publishing history. Datawatch, although I only have numbers back to DW5 - May 1989, has probably been in existence for almost as long as I have worked in recruitment. To mark the occasion I will provide a brief review of the main changes that I have seen in the recruitment market over the last fifteen years.

Certainly back then, names like Honeywell, ICL and IBM dominated. As centralised mainframe computing has given way to decentralised client server computing, MVS and VME have steadily been replaced on job descriptions by NT and the various flavours of UNIX. There has been a dramatic increase in the number and flexibility of programming languages and from a technical perspective the cost of computer power and capacity has fallen dramatically. Outsourcing is now a major feature and there is increased acceptance of external systems development. In recent years there has been a huge growth in web technology and the proliferation of e-commerce and corporate intranets.

One of the most common sentiments expressed in the recruitment market has been the supposed demise of computer auditors. On countless occasions I have been told by Chief Internal Auditors that they are no longer going to employ specialist computer auditors - all their internal auditors will now be able to undertake computer audit work. Without doubt general auditors have become more knowledgeable and have far greater expertise. I.T. however, has become more sophisticated and the specialist expertise that dedicated computer auditors provide remains just as important.

The type of work that computer auditors undertake has changed. Computer auditing, although predating the 1980's, emerged as a recognisable profession during the early part of that decade. Since that time computer auditing has moved away from reviewing existing applications and is now more involved in recognising risks and building controls into the management and development of new projects and systems. It has gained wide acceptance as part of the development process.

The backgrounds of computer auditors have changed. Fifteen years ago many computer auditors had technical backgrounds in IT. They had often come up through the programming and systems analysis route. At that time academic and professional qualifications carried far less weight in IT and for good or bad, many computer auditors in senior positions held educational qualifications that extended little beyond 'O' levels. It did them little harm in the recruitment market. That has changed. Many more companies, if they are to recruit externally, expect computer auditors to be, if not graduates, then professionally qualified. CISA and QiCA have become commonplace and will ultimately become prerequisites.

The number of dedicated computer auditors is falling. This merely reflects what has happened in internal auditing more generally and, to a lesser extent, illustrates that less specialist work can be undertaken by others. Certainly, many of the people who complete the CISA examination are not dedicated computer auditors. I would as a matter of course advise anyone planning to make a career out of internal auditing to do so. It is a very useful addition to your CV.

Computer audit departments, reflecting the internal audit departments within which they operate, have not only got smaller, they have got flatter. There is no longer a hierarchy of auditors, seniors, supervisors and managers.

Fifteen years ago very little computer audit work was contracted out. I would now estimate that at least 20% of all computer audit work is undertaken by external contractors. This could be anything from a Big 5 practice, where many computer auditors have more recently gained their initial training, to a specialist consultancy or not uncommonly, self employed practitioners. There is far greater flexibility in working practices and many computer auditors work under terms and conditions that they are able to negotiate for themselves.

For the greater part computer auditors have been in short supply. They remain so today. This has allowed computer auditors to be paid a premium, but they are regularly lost to positions in IT requiring a steady supply of new recruits. Unfortunately very few companies wish to take on the cost of providing initial training. This does little to enhance the supply relationship between computer audit and security has grown particularly in recent years. If the computer auditing profession was a product of the 1980's then security was a product of the 1990's. The two compete for staff and transfers in both directions have become common.

On the basis of the growth in the profession during the first 50 editions of Datawatch, there is no reason to assume that consolidation and maturity will not follow.

Back to Basics

A Control Framework for Spreadsheet Developments

Some years ago Datawatch published "The Subversive Spreadsheet, by RAY BUTLER which drew attention to the risks from spreadsheets. Since then a lot of work has been done by academics, developers and auditors in the European Spreadsheet Risks Interest group to gather anecdotal and empirical evidence of errors in spreadsheets, and provide guidance for developers and users of complex spreadsheet models. In this article, Ray brings us up to date.

An academic studying the business decision-making process recently told me that his early results indicate a potentially disastrous lack of knowledge by managers about the source (commonly a spreadsheet model) and quality (oh dear….) of the information they use for decision-making.

As CobiT is becoming the de facto standard for IT governance, I wondered if the principles behind it could be applied to something as intrinsically uncontrolled (some would say flaky) as a business' spreadsheets. It's encouraging to find that it certainly can - And here's how.

How does COBIT cover spreadsheet risks?

It doesn't - at least it makes no specific mention of Spreadsheets, or end-user computing. Instead, CobiT's framework covers all the principal IT processes. CobiT can be adapted, scaled and applied to IT solutions at all levels, from a whole Enterprise Resource Planning system to a (relatively) simple spreadsheet development.

Applying COBIT to spreadsheets

The control objectives (high level and detailed) and maturity model which follow show how the CobiT framework can be scaled to spreadsheet developments

The controls obviously need to be applied only as far as is justified by a spreadsheet's actual or potential impact on the organisation using it. A simple impact assessment has been described in Risk Assessment for Spreadsheet Applications (Proceedings of the First EuSpRIG symposium, July 2000) and will not be reproduced here.

High level control objective

Control over the process of developing and maintaining spreadsheet models and applications that satisfy the business requirement to provide accurate and error-free business models and analyses which effectively support the business process is enabled by the definition of specific statements of functional and operational requirements, and a phased implementation with clear deliverables, and takes into consideration

- Design Methods
- Security and data retention requirements
- Testing and Acceptance
- Documentation Requirements

Detail control objectives

- Design Methods

The organisation should employ a spreadsheet development methodology which requires that appropriate procedures and techniques, involving close liaison with model users, are applied to create the design specifications for each new spreadsheet development and to verify the design specifications against the user requirements.

- Major Changes to Existing Systems

Management should ensure, that in the event of major changes to existing spreadsheet models or applications, a similar development process is observed as in the case of the development of new models.

- Design Approval

The organisation's spreadsheet development methodology should require that the design

Table 1.

Maturity Level	Characteristics
0 Non-existent	There is no process for designing and specifying spreadsheets. Typically, spreadsheets are developed in an unstructured manner by untrained end-users, with little or no documentation of actual requirements and no testing. There is an extremely high risk of error in important spreadsheets.
1 Initial/Ad Hoc	There is an awareness that a process for developing spreadsheets is required. approaches, however, vary from development to development without any consistency and typically in isolation from each other. The organisation's business depends upon a variety of individual solutions with varying degrees of documentation and control and now suffers legacy problems and inefficiencies with maintenance and support. There is a very high risk of errors in important spreadsheets.
2 Repeatable but intuitive	There are similar processes for developing and maintaining spreadsheets, but they are based on the expertise within the users, not on a documented process. The success rate with spreadsheets depends greatly on individual users' skills and experience levels. Maintenance is usually problematic and suffers when internal knowledge has been lost from the organisation. There is a high risk of errors in important spreadsheets
3 Defined Process	There are documented development and maintenance processes. An attempt is made to apply the documented processes consistently across different spreadsheet developments, but they are not always found to be practical to implement. They are generally inflexible and hard to apply in all cases, so steps are frequently bypassed. As a consequence, spreadsheets are often developed and implemented in a piecemeal fashion. Maintenance follows a defined approach, but is often time-consuming and inefficient. There is medium risk of errors in important spreadsheets.
4 Managed and Measurable	There is a formal, clear and well-understood spreadsheet development and implementation methodology and policy that includes a formal design and specification process, a process for testing and requirements for documentation, ensuring that all spreadsheets are developed and maintained in a consistent manner. Formal approval mechanisms exist to ensure that all steps are followed and exceptions are authorised. The methods have evolved so that they are well suited to the organisation and are likely to be positively used by all staff, and applicable to most important spreadsheet developments. There is a low risk of errors in important spreadsheets.
5 Optimised	Spreadsheet development and maintenance practices are in line with the agreed processes. The development and maintenance process is well advanced, enables rapid deployment and allows for high responsiveness, as well as flexibility, in responding to changing business requirements. The spreadsheet development and implementation process has been subjected to continuous improvement and is supported by internal and external knowledge databases containing reference materials and best practices. The methodology creates computer based documentation in a pre-defined structure that makes production and maintenance very efficient. There is a very low risk of errors in important spreadsheets

specifications for all spreadsheet development and modification projects be reviewed and approved by management, the affected user departments and the organisation's senior management, when appropriate.

◆ Programme Specifications

The organisation's spreadsheet development methodology should require that detailed written specifications be prepared for each spreadsheet development or modification project. The methodology should further ensure that specifications agree with design specifications.

◆ Testing

Testing to ensure that:

- The spreadsheet calculations
- Data input and controls over data
- Links between host systems and the spreadsheet, between parts of the spreadsheet and between spreadsheets in a multi-file suite of models
- Output reports operate correctly and as specified according to the development test plan and established testing standards should be performed and documented before the development is approved by the user. Adequate measures should be conducted to prevent disclosure of sensitive information used during testing.

◆ User Documentation and instructions

The organisation's spreadsheet development methodology should provide that adequate user reference and support manuals be prepared (preferably in electronic format) as part of every spreadsheet development or modification project.

Security and retention

- The organisation's spreadsheet development and use methodology should include directions for ensuring that :
- Access to spreadsheet models is restricted to authorised persons;
- Spreadsheet models are protected against inadvertent or unauthorised modification
- Spreadsheet models and applications are retained in electronic form for the period of time appropriate to the purpose of the spreadsheet.

Maturity model

This maturity model measures how well a business meets the control objectives given above. In my experience it will make chilling reading for many of us....(see table 1).

Conclusions

As illustrated above, the CobiT approach can easily be applied to spreadsheets. Take a few moments to consider:

- How much your organisation depends on Spreadsheets for decision and operational support
- Where your organisation fits on the maturity model above.

If you have any number of high-impact spreadsheets and are at less than maturity level 4 you could be in BIG trouble (as a guide, the largest VAT error found in a spreadsheet in the last 12 months was around one million pounds). Consider two parallel courses of action.

First, review your procedures and see what you need to change to advance up the maturity scale for future and changed spreadsheet developments.

Second, consider testing and documenting the more important spreadsheets - Those which would cause your organisation real pain if they were wrong. Customs and Excise's SpACE spreadsheet-testing tool has recently rated "best of breed" in an independent comparative review.

You can get details from the author, or by emailing alastair.stewart@hmce.gsi.gov.uk

The leaves on the trees are turning brown and beginning to fall, summer is over, autumn is upon us, so it must be CISA results time.

I would like to take this opportunity to offer my congratulations to this year's successful Central Chapter candidates. The top three scores are: 1st, **Mitch Henderson**, 2nd **Geoffrey Dale**, joint 3rd **Marie Anne Byrne** and **Philip Godwin**.

The other successful candidates are: **Stewart Carter**, **Jennifer Duncan**, **Kevin Lally**, **Jane Newboult**, **Ian Rankin** and **Andrew Wildgust**.

This is the time of year when we look forward to the year ahead, the committee is hard at work planning next year's events, and we would welcome any suggestions you may have for topics, speakers or venues. The committee has decided that as we are a technology group we should be promoting the use of technology more. With this in mind, we plan to reduce the amount of paper we send out, therefore we are looking to send out the majority of information about future events by email and posting the information on our web site. So please regularly check the web site for the latest information about Chapter events.

It is also that time of year, I'm afraid, that you need to renew your membership subscription. This year I am sorry to say, and after much deliberation, we have had to raise the Chapter dues portion of your subscription by $20, from $35 to $55. The Chapter dues is the amount of your total international subscription that we as the local chapter retain. This is the first time in several years that we have made an increase in Chapter dues, but the committee felt that we could no longer absorb rising costs. This rise in Chapter dues will cover the increasing cost of administration and the additional cost of Datawatch.

I often get asked the question of what is good IS Governance all about? To me IS Governance is exploiting the full benefit of using IS/IT, together with identifying and understanding the associated risks and effectively managing these risks.

At an operational level I think this is well illustrated by some recent work I have been involved with at a higher education institution. I was tasked to assess the University's management arrangements for virus protection. The results of this work clearly demonstrate the need for effective corporate governance. First of all you need to understand the organisational structure of a traditional higher education institution. Generally there will be a central administration function focusing on HR, Finance, Marketing, etc together with a central administration IT team. Then there are the individual academic facilities and schools, who have devolved management responsibilities, and more often then not, their own small IT team. The results from our work identified that there were some good pockets of anti-virus management practices in place, particularly in the central IT area, but there were also several areas of the University where anti-virus protection required, shall we say, some improvement !!

The biggest failing was that there was no one central entity responsible for anti-virus protection across the whole of the University. Therefore we found an inconsistency in approach, good protection in some areas and poor controls in others. The areas of poor control, however undermined the areas where good controls were in place.

I had also led a number of other assignments at the University, looking at software licensing and network access, and a common theme was emerging, there were pockets of good control here and there, and lack of control in other areas, and there was no one entity taking a corporate view. The University as a whole was being exposed to vulnerabilities due to the inconsistency of applying appropriate and effective controls.

The main problem I faced was not the technical issues of the assignment, but the University's culture. Many of the line managers, whilst agreeing with the fundamental findings of my work, were of the opinion that this is the way the University is managed, and had been for decades, so it was impractical for a corporate view to be applied across a devolved management structure.

Fortunately the Audit Committee meeting where I raised my concerns of the lack of corporate governance was attended by the Vice Chancellor (VC), who quickly picked up on the importance of this issue, that the institution was seriously exposed and that potentially the institution's reputation could be seriously damaged. Higher education institutions value and protect their good reputations, as it is this that attracts the best academic staff, the best students and research grants. The VC stated that this area was too important not to consider making radical changes in the way the University was managed, but in such a way that a corporate governance framework could be established, whilst maintaining the flexibility of devolved management.

Corporate governance and in particular IS governance is now very high on the agenda of both the University's Audit Committee and senior management.

The above example clearly shows that we, as internal audit and risk management professionals, need to take a step back from our day to day work and not get too wrapped up in the detail of individual assignments, we need to take a higher view to understand the 'bigger picture'. Therefore we can identify corporate, and in particular the IS governance issues, and continue to raise these issues at every opportunity and at every level within our organisation.

ISACA's International Office What do they do there?

At the last London UK Chapter AGM, one of the questions raised related to the part of our membership subscription that goes to International Office. For the coming year 2002, this will be $115, a high proportion of the total subscription whichever of the UK Chapters you have joined. In the following article, LYNN LAWTON sets out what we get for that money, and we hope you will agree that it's a good deal.

First of all, International Office itself is in the north west suburbs of Chicago, between 30 minutes' and 2 hours' drive from "downtown", depending on who is driving and how much it is snowing (it's always winter when I go there). The ISACA office takes up most of the 10th floor of a purpose-built office block. Far from luxurious, it houses 43 staff in fairly cramped conditions. While the name Rolling Meadows may convey the image of a country idyll, there is in fact not a meadow, either rolling or stationary, anywhere in sight. A few office blocks, a hotel, bungalows and wide roads with no pavements (no one walks anywhere) are the principle features.

The International Office staff deal with emails, faxes and telephone calls from all over the world, from members, prospective members and the multifarious other organisations with which ISACA works. They are under constant pressure to respond speedily and professionally. They are as much the public face of ISACA as are we, the members.

Their work falls into 5 main categories:

- membership
- education (e.g. conferences)
- certification (CISA)
- publications (e.g. CobiT)
- research (e.g. the Technical Reference Guides on e-commerce controls, audit and security)

With the exception of research, each category aims to be at least self-funding and is not subsidised by the other operations. The breakdown of revenue and costs for the last financial year (to 31 December 2000) is shown in the following graph.

The membership subscriptions cover the following activities:

1. Information Systems Control Journal

The membership benefit most visible to all of the members is the publication and distribution of 6 volumes annually of the Journal. This is packed with practical advice, up-to-date news, book reviews and information on new developments in the security and controls arena. It has, on many occasions, been invaluable to me in talking to clients about current issues around their forays into new technologies and software. The fact that I have a complete library from when I first joined ISACA, and still refer to the back numbers occasionally, says a great deal about the quality of the material - and about my hoarding tendencies. In my view, this publication is, by itself, worth the cost of the International subscription.

2. Global Communique

Another bi-monthly publication for all members. This keeps you abreast of what is going on in ISACA and its chapters around the world.

3. Discounts

Members get substantial discounts on ISACA's research and other publications, conferences and CISA examination fees. This gives everyone an incentive to take advantage of a superb range of educational and research material that is directly relevant to their field of expertise.

4. Knet

Speaking of superb ranges, check out ISACA's

Knowledge Repository at isaca.org/knet. Although still in its infancy, it already sports a vast amount of information, including Journal articles, audit programmes, book reviews and other tools.

5. Thought leadership

As well as getting direct personal benefits from the research and other publications, members can use the open standards published by ISACF and the IT Governance Institute to benefit their organisations. As an ISACA member, you are part of an organisation that is leading the field in IT governance and security, as demonstrated by our recent publications "Board Briefing on IT Governance" and "Information Security Governance: Guidance for Boards of Directors and Executive Management". Introducing these documents to your organisation will enhance your own profile, as well as that of the IT Governance Institute.

6. Chapter support

Less visible to the membership at large, but no less valuable, is the support provided to all Chapter boards by International Office. Comments at the Chapter AGM's I have attended indicate that you all recognise the tremendous amount of work that your Chapter boards put into providing an active local forum for networking, education and knowledge sharing. International Office assists them with these activities by providing advice, templates and a forum for discussion and sharing of experience. Examples include:

- Conference calls and a few face to face meetings of the International Membership Board. This is a group of representatives from Chapters around the world. It exists to provide input on ISACA's membership ideas, based on their familiarity with member and chapter needs. It also supports chapters that are in difficulty and assists in the development of new membership programs for chapters and members.
- Printing and distribution of subscription invoices, and collection of payments
- Leadership conferences, where Chapter presidents get together to share with each other their successes (and occasionally their failures) so that the whole ISACA community benefits from new ideas
- A monthly chapter newsletter, that also contributes to this knowledge sharing
- Membership recruitment packs and advertising
- A chapter administration manual and success guides, so that no one has to start from scratch, whether they are setting up a new chapter or designing an events brochure.
- Exit surveys, so that we know why members leave
- Regular statistics, so that the Chapter boards can keep track of how their membership compares with that of other chapters. This can be very competitive!
- Translation services, so that members who do not speak English do not lose out on the many benefits of ISACA membership.

7. New member packs

Each new member receives a pack of information, including ISACA's IS Auditing Standards and a copy of the CobiT Executive Summary and Framework.

8. IS Auditing Standards and Guidelines

As an ex-chair of the Standards Board, I know how much effort goes into developing our standards products, and how useful they have been to me in carrying out work in new areas. The Standards Board exists to define, develop and promulgate IS auditing standards and their associated interpretations and guidelines, and to maintain a liaison with other standards bodies. Membership costs include the monthly conference calls and two face-to-face meetings of this small international group.

9. Academic Relations Committee

The Academic Relations Committee's conference calls are also funded from our international subscriptions. This committee exists to provide a framework for information exchange between, and for the mutual benefit of, the Association, the business community and the academic community. Our new members will come from current University students, and the earlier we can introduce them to the benefits of ISACA, the more likely they are to join and become our ambassadors of the future.

That is a brief summary of how the international element of your subscription is spent. However, this is not a picture that stands still. Cost statistics for non-profit-making organisations similar to ISACA are readily available, and are used regularly to benchmark the performance of International Office. ISACA's Activity Based Costing Module indicates that while there is an overall small surplus of revenue over cost per member, this comes entirely from the new member administration charge, which subsidises the cost of supporting renewing members. So ISACA is vigilant in seeking ways to deliver its services to members more efficiently and effectively. You will have noticed, for example, that more of the publications are becoming available on-line, with a view to cutting back on the cost of printing and postage in the long-term. A new computer system is also being sought to enable a move to taking payments on line, and providing even more services across the web.

We have not yet reached a state of perfection, nor indeed are we aiming for that. We do, however, aim to provide value for the international subscription cost, and I hope you now agree that you get it.

Lynn Lawton, CISA
International Vice President, ISACA and
Director, Information Risk Management Services, KPMG London

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
http://www.pki-page.org/
http://www.microsoft.com/TechNet/win2000/win2ksrv/prodfact/pkiintro.asp
http://www.sans.org/topten.htm
www.securitywatch.com

COMPUTER COMPANIES AND SYSTEMS

www.microsoft.com
www.alw.nih.gov
ntresearch.com/
www.acl.com/audit/audit2.htm
www.caseware-idea.com
http://www.sap.com/mysap/
www.windowsitsecurity.com

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

Answers to Word Puzzle on page 3.

Cere, Coerce, Come, Comer, Commerce, Cor, Core, Corm, Crème, Croc, Ecce, Eer, Emmer, Ere, memo, Mercer, Mere, Mom, More, Oer, Orc, Ore, Recce, Ree, Rem, Roc, Roe, Rom.

[All words from Concise Oxford English Dictionary]