ISSN 1356-0735

AWARD WINNING

DATAWATCH

VOL. 45, JUN-SEP 2000

IN THIS ISSUE:

THE QUARTERLY MAGAZINE OF ISACA LONDON CHAPTER

VOLUME 45 JUN-SEP 2000

DATAWATCH

is a quarterly magazine
published by the

Information Systems Audit and Control Association

London Chapter

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

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

In this issue:

FEATURES

REGULARS

PLUS

ISACA London Chapter Committee 1999/2000

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

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

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

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

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

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

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

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

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

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

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

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

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

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

STANDARDS
Joseph Wright
Credit Commercial de France
0207 334 3591
joseph.wright@ccf.co.uk

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

ISACA Northern UK Committee (officers only)

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

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

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

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

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

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

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

WEBSITE:

WWW.ISACA.ORG.UK/NORTHERN

ISACA Central UK Committee (officers only)

PRESIDENT
Mike Hughes
KPMG
0121 232 3207

VICE PRESIDENT/CISA
Simon Parker
Canada Life
01707 422064

SECRETARY
Steven Babb
KPMG
0121 232 3213

TREASURER
Geoff Adey
KPMG
0121 232 3202

PAST PRESIDENT
James Whittaker
BT
0121 230 2214

WEBSITE:

WWW.ISACA.ORG.UK/CENTRAL

The Editor's Chair

By Annabel Lane

Welcome to another edition of Datawatch, where once again the theme is that of Ecommerce. Not terribly surprising I suppose as it continues to be given a great deal of column space by the media and despite some worries and spectacular failures, the general trend is still onwards. I am sure not many of us work for companies who don't have their own web site by now, and many are utilising ebusiness in one way or another, for procurement for example, or facilitating customer communications.

The London Chapter of ISACA, as you know, is no exception and I hope most of you have visited the Chapter web site and found it useful. Of course, under the guidance of our extremely pro active web master, Allan Boardman, we are constantly trying to improve the web site as a service to you, the members. Well, that's what it is, after all, and we are always happy to receive any suggestions or feedback on this as well as any other area under the control of the Publications Committee. We were recently asked at the Chapter AGM whether we were considering putting Datawatch itself on the web site. Well, that is a question that has been debated long and hard at more than one committee meeting, and we all see the merits that making Datawatch available in this manner would give to the members. But therein lies the rub; our magazine is a service to fee paying members and the Committee in their wisdom have always thought that to publish it on the web site would negate this benefit if it were possible for all and sundry to read it. That is the main reason this has never been done. However, if we were able to create a private area on the web site for members only, then I think we agree that this would be a very good way to make Datawatch articles available over the Internet. That is one of the areas our web master is currently investigating (along with several others). However, following a request from a member, we are hoping to be able to make a partial solution available in the near future. It has been suggested that we might be able to post at least the titles and subjects of articles that had appeared in Datawatch so that visitors to the site could search for a subject that interested them, find out which edition it had appeared in, and go about getting hold of the relevant magazine. Again this is something that Allan is working on at present, but it is a service we hope to provide. Other possibilities that have been suggested have been a discussion forum and a type of bulletin board. If you think you would - or wouldn't - use any of these services, we are happy to hear from you. After all, if we don't hear what you want, we have to guess and we may be wrong! So if you have any comments, feel free to contact me, or any other member of the Publications Committee.

Mind Games
by Puzz

The answer to each clue is a word which links with each of the three words listed. This word may come at the beginning (e.g. ODD linked with BALL, FELLOW and SOCKS), at the end (e.g VILLA linked with ROMAN, ASTON and HOLIDAY), or a mixture of the two (e.g. AGE linked with BOND, BRONZE and GAP). Once you have solved all the clues, take the first letter of each word and rearrange them to form a word well-known to us all. Answers on page 28.

1. PLAY	MAKER	SAFETY	.....	5. JACK	STRAP	LEG	.....		
2. SIDE	RACE	RAGE	.....	6. SPEAK	OVER	CHAIR	.....	9. HAND	DRIVE	TAKE	.....
3. CROSS	THROAT	LASS	.....	7. SPOT	DRIVER	CONS	.....	10 LODE	ROVE	AIRED	.....
4. GRAND	NET	PAR	.....	8. LING	STAND	WELL	.....				

From the President

By John Mitchell

The recent start-up problems of the Internet banks Egg and Cahoot have more than just their funny names as a common cause.

Although at the time of writing the only explanation offered is along the lines of 'unprecedented demand', this is really systems speak for 'we did not do adequate capacity planning'. Capacity planning, or to give it its more sexy name of configuration management is something that many organisations play lip service to, but which seldom gets done in practice. The reason for this, apart from laziness and the obvious technical complexities, is the new mantra of 'power is no longer a problem'. I first heard this chant some eight years ago from the president of Microsoft UK who stated that the Wintel combination meant that designers no longer had to concern themselves with lack of power as chip speeds were doubling every eighteen months. He completely ignored all the others components of an installation such as data transfer, network capacity and the built in inefficiency of code generated by visual basic, but that was becoming par for the course. I came across this in reality about six years ago when reviewing a system development for a commodity trading company. I ascertained what the system was required to do and in what time period and concluded that the users required a real-time response time of about half a second at their workstations. I then found the proposed configuration details, but could not find the supporting data. I then asked the obvious question and was told that in the experience of the project team the configuration was correct to 'an order of magnitude'. Having thus established their interest in astronomy I enquired if they knew the difference between a star of magnitude one and another of magnitude two. After initial blank looks they hazarded a guess of 'twice as bright'. When I corrected them to one hundred times as bright they pointed out that even if they found they needed a hundred times more power they would just go and buy a bigger box. I then raised the twin spectres of data transfer rates and network capacity and suggested that they ask an expert to size the system for them - just to be on the safe side. They did not know of any such expert, but I knew a man who did and asked for a quotation for doing the work. The price came to £3,500, which was turned down by the project manager as being excessive (the total budget of the project was £1 million!). The system eventually went live and ran like a dog. They could not purchase more power immediately because they already had the biggest Wintel machine that money could buy. Not that raw power was the problem, it was the network that was the bottleneck. Moral of the story? Plan hard, work easy.

ANNUAL GENERAL MEETING
18 MAY 2000

PRESIDENT'S REPORT

I apologise for not being able to give this report myself and I am grateful for the Vice President volunteering to present it on my behalf (and also to field any questions!). I make this report on behalf of the entire Committee, but any omissions, or inaccuracies, are as a result my poor memory and not as a result of any shortcomings of the members of your Committee. This report covers 1999, but as that is now so long ago, please forgive me if I bring in a few more recent events.

It is with pleasure that I am able to report that in 1999 the Chapter exceeded 650 members for the first time. We are the second largest Chapter in the world with only New York Metropolitan being bigger. We are also one of the most active with our programme of events far exceeding that offered by other Chapters. We are also financially, sound as will be described later by our Treasurer.

Our programme of ten, free late afternoon events is widely perceived as providing some of the best training available to IS auditors in the southern part of the UK. This is coupled with our chargeable training programme, which pound for pound provides by far the most cost-effective delivery of technical matters to be found in the UK. Taken

together, these aspects of our Chapter service provide the capability of keeping IS auditors up to date on a wide range of issues and also enable those with the CISA designation to obtain the relevant CPE hours. Our events are handled by Steve Bailey and Karen Sharpe, supported by Jackie Bowles of KPMG for our evening events. My thanks to all three.

Over half of the Chapter are now CISA qualified and our annual CISA Review Course, administered by David Spaven our CISA co-ordinator, is always well subscribed. On average over 100 people from the Chapter take the exam each year with about twenty percent attending the review course. On average, the success rate for the Chapter is about eighty percent as against a worldwide average of just fifty-two percent. Derek Oliver, a past President of the Chapter and a current Committee member, is actively involved in setting the examination (so you know whom to blame!)

Apart from our monthly mailshot, which keeps you informed of forthcoming events, our quarterly magazine, Datawatch keeps on winning awards for best 'newsletter'. One of the reasons that we do not call our mailshot a newsletter is because it confuses International when they come to judging the various 'newsletters'. Datawatch is so far ahead of the crowd that I have had requests from other Chapters to be included on the circulation list. Something that we may consider if we can sort out a suitable charging structure. The success of Datawatch is in no small part due to Annabel Lane, John Hunter and Bill Hawkins who comprise the editorial team. You should also have noticed that our web site has improved in content and presentation due to the efforts of Allan Boardman, our Web Master.

John Hunter and Bill Hawkins provide support to our various Special Interest Group (SIGs). The SIGs are fairly autonomous in that they run their own programme of events under the Chapter umbrella, but with John and Bill providing the necessary guidance. The Chapter currently has three active SIGs. The Network SIG has been established for three years, holding some four to five meetings per annum. The Fraud Prevention SIG and the Risk SIG have recently been formed with inaugural meetings in the last few months.

Kamal Khan is on the International Research Board and also provides the Chapter link to the various UK universities that offer IS Audit courses. During 1999 the Chapter received an award for its support on the digital signatures project, which was in no small measure due to the amount of work put in by Kamal to make the resulting publication such a success.

Kamal is also responsible for membership liaison and those of you who forgot to renew your subscription will have received a gentle reminder from him.

Archie Watt our Treasurer keeps a careful eye on our income and expenditure and will be reporting separately on the state of our finances. Some of you may remember that a few years ago the Chapter suffered a financial crisis, but with Archie in charge there is no chance of that every happening again. Having been in the Treasury hot seat myself I know that it is one of the more demanding roles on the Committee and my thanks to Archie for discharging the role with such efficiency.

We are one of the few Chapters to have a paid, part-time administrator, but we found some years ago that we could not administer such a large Chapter on a volunteer basis. Nancy Watt runs the Chapter office on a part-time basis and Charles Mansour provides the formal secretarial support to the Chapter, including the management of our monthly committee meetings. My thanks to both Nancy and Charles for their efforts.

Gerry Penfold, a past Chapter President provides me with calm and sound guidance when things get fraught, as they so often do when attempting to juggle the requirements of member service and financial stability. Gerry is a partner with KPMG and the Chapter relies very heavily on support from KPMG for hosting both the Committee and the events evenings. Likewise, BDO, via Archie Watt provides us with use of their training facilities for our chargeable events, including the CISA review course. Deloittes & Touche, via Karen Sharpe kindly hosted the annual Committee dinner, which is the once a year reward that we offer ourselves, at no cost to you! All these organisations ask nothing in return for what they provide. This pro bono support is most welcome and my thanks to both KPMG, BDO and D&T for all the help that they provide and without which our membership dues would have to increase considerably.

The Chapter is on a firm financial footing and with the administration processes now in place I consider that our ability to service our members has never been better. This does not mean that I am complacent and I will constantly strive to provide you with the best level of service that is possible.

Internet Fraud and Vandalism

By Karen Nelson, Insight Consulting

In the rush to deploy Internet and Intranets, businesses often fail to take simple steps that would reduce their vulnerability to attack or fraud.

Microsoft Internet Information Server 4.0 and SQL Servers 6.5, and 7.0 are popular platforms for deployment that have well publicized vulnerabilities. This article explains how you can ensure that IT closes the security gaps in its web based deployments.

Threats, Vulnerabilities, Incidents

The first step in auditing security of Internet based applications is obtaining management's agreement on the importance of the site to its business through risk assessment. Depending on the business objective for the site, many Intranets would probably be considered of low to medium risk, that is important but not critical. Extranets and E-commerce sites may be considered high risk, meaning that loss of information will impair business operations to such an extent that customer services and products cannot be provided. Performing a risk assessment provides an opportunity to enlighten business managers on the sensitivity of information and systems requiring protection, according to the Information Security Forum. This is done through business impact analysis, threat analysis and security control selection. This also is a good time to make business managers aware of reported incidents and the consequences of their occurrence.

The LoveBug virus, not including its predecessors, is said to have infected over 600,000 machines and cost American business $2.5 billion. The February 2000 distributed denial of service attacks (DDoS) that hit major providers such as Yahoo, eBay and Buy.com were estimated to have cost businesses $1.2 billion. Last year reports from the Association of Payment Clearing Services' showed an 11% jump to £135m in fraud involving remote transactions - those over the Internet, by mail order and phone - (the organisation did not yet distinguish how much of the fraud is due to Internet transactions). The Institute of Chartered Accountants expects online fraud to grow to £5 billion a year.

In January "Maxus," a hacker stole credit card numbers from an online music seller and attempted to blackmail the company, make fraudulent purchases, and finally offer the card numbers for sell over the Internet. In March 2000 a software consultant reported to MSNBC how its firm was able to retrieve 25,000 credit card numbers from 20 web sites by exploiting a commercially available database tool rather than web browsers. These sites used Microsoft SQL Server. You won't believe how simple it was to break in (explanation to follow). Along with credit card numbers hackers may obtain personal information about customers, including name, address, and social security numbers.

Steps to Prevent and Respond

Before you can adequately plan security of the site, you need to clarify the organization's goal for the site in terms of risk. How would a loss of confidentiality, integrity or availability from this application impact the business? What are the most likely threats that would cause these events to occur? This information can be used to develop security standards and Internet policies for the site. Microsoft has released numerous technical guidelines for implementing appropriate security controls in its products. A summary of the control options to check is presented in Table 1 (see over), followed by a description of key controls.

Simple Controls

How could it be so easy to retrieve credit card numbers from Microsoft SQL Server? The server had no password protection on their databases or had password information exposed on their web sites. The installation program for SQL Server 6.5 and 7.0 leaves the superuser account 'sa,' with a blank password and the administrator must manually change this. A registry entry exposes the sa password in clear text. Another account that may be exploited is the SQL "guest" account. A poorly designed application may utilize the guest account to provide access to any user, even those without an account. Therefore, if one wished to establish a connection to the database, it would be easy to exploit any of these weaknesses.

Delegation

While these gaps are fairly easy to close, others are not. When deploying IIS Server and SQL Server on separate servers, another problem prevents the use of integrated NT 4.0 NTLM authentication. This problem is known as delegation. Normally When an Internet user makes an HTTP URL request which requires access to the SQL database, the IIS Server authentication routine is invoked. The IIS server routine would attempt to match an encrypted token from the

Table 1. Microsoft IIS and SQL Security Control Options

Security Requirement	Control Options
Authentication & Identification	Check for the type of authentication in use [Note: different authentication methods can be set at the sub-directory and virtual server layers]: * If Anonymous access, place public files in separate directory and use NTFS and ISS browser permissions to restrict access to READ * If Basic HTML access (clear-text password), check for the use of SSL during authentication to protect password during transmission * If NT Challenge Response authentication using operating system accounts, check password management settings, encryption level, and use of shared user accounts * If Public Key Certificates are mapped to NT accounts, check for valid certificates and verify that client browsers recognize revoked certificates. * If bespoke authentication modules are used, look for the use of hard-coded generic passwords. * For sites using user accounts, verify that password was changed within 90 days or less. * Check for registry permissions on password information, particularly the SQL 'sa' password. * Check authentication components of third party tools, such as VPNs and firewalls. * Verify password management features, including strong encryption as required. * Set a very strong Administrator password, of 9 characters or more. Have administrators use individual accounts. * Disable guest account.
Access Control	* Verify NTFS file permissions of READ only on content files, SCRIPT OR EXECUTE on executables and script. * Verify appropriate IIS Web Server permissions: read, write, script and execute, list or browse. * Remove or restrict use of special privileges, such as debug * Obtain documentation of application and Transact-SQL statement permissions and verify appropriate permissions. * Verify SQL user and role permissions * Verify password-protection with an appropriate account of ODBC connections * Remove unused or unauthorized ODBC and OLE connections * Restrict use of default accounts according to the principle of least privilege. * Allow network-only lock out for Administrator account * Remove Net Shares * Set Registry permissions * Provide confidentiality and integrity with third party tools, such as SSL communications, VPNs and firewalls. * Ensure developer debug options are disabled.
Audit and Accountability	* Configure NT event logs and performance monitoring, which utilize audit, IIS, FTP and SQL statistics * Enable NT auditing * Configure SQL auditing * Configure Site Server Express for reporting of audit logs and verify procedures for reviewing and archiving logs.
Environmental	* Display legal notice before login * Ensure service packs, hot fixes and patches are up-to-date and security utilities applied. * Install minimal IIS Services required * Remove or disable services that are not required * Move (to private directory), remove or disable critical files, including DLLs and EXEs that are not required or should be restricted * Configure TCP/IP to deter DoS attacks * Configure metabase and registry appropriately * Verify ISP contract meets or exceeds requirements * Provide physical security for servers
Backup & Recovery	* Determine Availability requirements * Develop backup & recovery strategy (not all ISPs provide backup) * Ensure safekeeping of backup medium

client with an encrypted token from the Domain Controller. The encrypted tokens are generated separately by the client and the domain server using the username, domain name and a password hash generated from a randomly generated key supplied by the IIS Server. The IIS server receives both tokens and expects them to match. When matched IIS can impersonate the authenticated user during the session. However, when the request is for access to an SQL database on a separate server, IIS does not have a valid username and password to authenticate the request - it only has the password hash in the form of an encrypted token. In other words, IIS is not able to delegate authority. This limitation can be stated as, "resources that require NTLM authentication in order to be accessed will not be able to access resources on another physical NT machine." Resources includes ASP Scripts, Active X Objects, Visual Basic and SQL connections. With the introduction of Kerebros in Windows 2000, the inability to delegate during authentication is no longer a challenge to integration of IIS and SQL Server on separate machines. [SQL Server 7 can use Kerebros authentication.]

However, to get around the problem of delegation in NT 4.0 and IIS administrators will configure an untrusted TCP/IP connection and use basic authentication. If access controls are not configured on files and scripts, access is allowed to Everyone. If a database uses a guest account or assigns permissions to the PUBLIC role, any request attempting to access the database can gain entrance. More secure options for using SQL server are available, and SQL 7.0 has new features which provide stronger security measures.

A good solution is a configuration used by the administrators on http://www.NTSecurity.net. The site uses two network cards in its IIS Server - one card is used for Internet-originated Web client requests over TCP/IP; the other handles only authenticated Named Pipes queries to the SQL server. The administrator created a business database separate from the system databases and tables. He created a special account to use for SELECT (view) only querying against business application tables and did not grant the account modify, add, or delete records in any of the tables.

SQL Server 7.0

SQL Server 7.0 supports application-level security and other new features that make it easier to implement security controls.

While SQL 6.5 supported three forms of authentication: Standard, Integrated and Mixed Mode, SQL Server 7.0 supports only Integrated and Mixed Mode. Integrated security requires the use of the Named Pipes connection protocol and NTLM authentication. Standard Security requires the use of an untrusted connection protocol, such as TCP/IP, and requires its own logins and user accounts for access. SQL Server 6.5 uses groups to assign permissions, SQL Server 7.0 uses roles.

"Integrated Security" became "NT Authentication Mode" in SQL 7. A NT user or group account can be added to the SQL server login tables as an externally authenticated account. When the client connects, the SQL Server checks its system tables for entry that matches the client's account. Non-trusted or Internet clients only should connect using Mixed Mode.

After a user is connected to the database, the user cannot access the database unless granted specific access permissions through the account or roles. Each database within SQL 7 has two default user accounts: Database Owner (dbo) and guest. The sa login account and members of the System Administrators role are mapped to the dbo account. The dbo account cannot be dropped. The guest account allows SQL logins without user accounts to access a database. The guest user can be added or dropped from any database except the master and tempdb databases. The guest account has no privileges by default except through its membership in the public role. When databases grant permissions to Public role, all users will have those permissions. SQL 7 has seven fixed server roles that provide the highly privileged access required of dba's, system administrators, operations staff and security administration. Assignment of these roles to users should be restricted based on job requirements.

SQL 7 permits managing application security with views and stored procedures. Users can be granted limited privileges on views without affecting the underlying tables as long as the view and the table have the same owner. Users can be granted execute on Stored procedures without granting them access to tables that are read or modified. Only applications that are written to execute the stored procedures will gain access to the data.

Another way of ensuring that users gain access to data through a specific application only and not another product such as Microsoft Excel is by using application roles. The user activates the application role by invoking an application, not by direct grant of a permission. The application role is protected with an encrypted password. The activated application role overrides the user's other permissions in the database regardless of other grants to the user. This makes it easier to restrict user activity in the database, however, it requires utilization of change controls over the applications and the application roles.

Other procedures and configuration options must be reviewed to ensure baseline security standards are met and vulnerabilities eliminated. These include network controls, as well as server-based options. Many incidents may be avoided by ensuring that service packs, patches and hot fixes are up-to-date.

Karen is a consultant specializing in database security. She is a CISA, CIA and a Certified Microsoft Professional. She is a member of ISACA and the IIA. She has worked in information security and audit for the past 12 years for several Fortunes 500 companies and non-profit organisations.

CISA for the New Millennium

By Derek Oliver, CISA

Many, many thanks to those of you who responded to the Certification Board's Questionnaire seeking information to help us design an new CISA examination.

At the April meeting of the Board, we were presented with a mass of information by our testing agency, Professional Examination Services (PES); it took us 4 days to gather it together, understand it and produce a new CISA design for the examination. Our task is to make sure that the CISA designation continues to represent our profession and that the examination reflects current practice and technology, in short, what an IS Auditor at the three to five years experience level does today.

First, a few background statistics. The questionnaire was sent out on a sample basis to 1,000 CISA-registered IS Auditors right across the world. In the period 1997 - 1999, 25% of all new CISA registrations were from Region 3, which includes the UK Chapters; for this reason, 230 questionnaires (23%) were sent to members in our region. The response rate from the UK was 32%, one of the highest in the region.

The sample selected crossed many boundaries, not just national but job descriptions, years of experience and field of employment. For instance, 26% went to people in the IS Auditor (Internal) category, 51% had 6 to 10 years IS Audit experience and 27% worked in the financial sector.

The questionnaires, which should have taken about an hour to complete, listed a number of tasks across the old CISA domains and asked, for each, the frequency the task was performed, the criticality with which it was regarded and what level of staff performed it (from IS Auditor with <5 years up to IS Technician). Some very interesting concepts appeared when the responses were analysed.

CAATS, for instance, were found to be rarely performed and not regarded as critical; perhaps this is due to the modern "Audit Tool" approach ? Similarly, the old favourite of Auditors, Statistical Sampling appears to be old hat too. We were also surprised to note that evaluation of encryption, at least in its technical form, was infrequent and non-critical. All of this caused us to look very hard at the pool of questions we use to set the annual exam and make sure that we were not asking too many questions in these, and other areas.

In terms of what knowledge an IS Auditor needs to do their job, overwhelmingly Security Management Techniques, Logical Access Controls and Business Risk Analysis came across as being the most important areas on which to concentrate.

So, where will CISA 2001, and for a few years thereafter, be concentrating? You'll be hearing more complete details from ISACA's Director of Certification, Terry Trsar in due course but below you'll find a brief, high level review of the new structure. Incidentally, the Cert' Board have had to go through every single one of the 600=odd questions in the 'pool' to reallocate their domain (we call it their "rubric").

This exercise identified many areas where we are very short of questions, like some tasks require, e.g. 4 questions in each exam to match the statistical requirement arising from the questionnaire, but we only have 4 in the pool. Item Writers are being informed where shortages lie and are asked if they would concentrate on these. Of course, we always need more items, and more item writers so CISA's out there, drop an e-mail to cisa@isaca.org and ask Kim Cohen for an Item Writer pack - remember every question accepted by the Test Enhancement Committee (TEC) gets you US$50 !

The new structure is in 7 domains, 6 "content" and 1 "process" based, they are :

1. Management, Planning & Organisation of Information Systems - Evaluate the strategy, policies, standards, procedures and related practices for the management, planning and organisation of IS.

2. Technical Infrastructure and Operational Practices - Evaluate the effectiveness and efficiency of the organisation's implementation and ongoing management of technical and operational infrastructure to ensure that they adequately support the organisation's business objectives.

3. Protection of Information Assets - Evaluate the logical, environmental and IT infrastructure security to ensure that it satisfies the organisation's business requirement for safeguarding information assets against unauthorised use, disclosure, modification, damage or loss.

4. Disaster Recovery & Business Continuity - Evaluate the process for developing and maintaining documented, communicated and tested plans for continuity of business operations and IS processing in the event of a disruption.

Continued on page 21

NETWATCH

By Annabel Lane, Nestle UK Ltd

Despite the recent rough ride that shares in the so called "dot com" companies have been having recently on the stock exchange, with flotations being postponed, and the first "e-casualty" in the form of boo.com, the interest generally in Ecommerce appears to be continuing unabated and we as auditors are still being asked to put in our two penn'orth to the projects our companies are running.

Well, either that or we are having to find out what is going on and make sure we get to add our input. A glance at this edition of Datawatch will confirm that this is still a hot topic, and so I thought it appropriate to use this edition of Netwatch again to have a look at what some more useful sites on the web.

http://ecommerce.internet.com/

I liked this one so I thought I'd kick off with it. It's run by Ecommerce Guide.com, who are sponsored by MySAP.com, SAP's new ecommerce initiative. There is a link in the top right hand corner to their site, which I expand on further below. This is such a large site with so many links that I don't really know where to start. The middle of the page has a list of "what's new" articles. When I visited the top story was an informative one on WAP, what it is, who is likely to provide it, what it's constraints are, and, if you have a liking for all things techie, even down to the nitty gritty of the WAP protocol stack and how it works. On the right hand side, there's ecommerce news and below that the opportunity to participate in discussion forums, sign up for newsletters, and even search in a "webopedia" to clarify some of the jargon over enthusiastic techies are wont to use. The left hand side contains links to a huge amiunt of other sites, ranging from portal sites, to information on ecommerce tips and trends, a library of resources and including links to other internet commerce sites. For example, clicking on the library link to security items takes you to another page containing latest news items in this area. I would recommend you to log onto this one and have a look around - definitely my star site of the edition.

http://www.sap.com/mysap/

I include this as I know there are a lot of you out there, who, like me are SAP users. MySAP.com is SAP's new brand almost, a new initiative to push ecommerce aspects, which they call collaborative, or c-business. Makes a change form ebusiness I suppose, but trust SAP to be different! It sets out how SAP aims to deliver business benefits through MySAP.com: There are 4 main elements:

1 Marketplaces - E-business hubs on the Internet that provide a collaboration infrastructure;

2 Workplaces - Enterprise portals which aim to increase employee productivity by facilitating access;

3 Business Applications - e-Commerce, Customer Relationship Management, Supply Chain Management, etc., and

4 Application Hosting - to reduce the risks and investment requirements of smaller companies. Clicking on the Ebusiness solutions button on the left hand side gives you access to a page with links to information on a lot of SAP initiatives such as Customer Relationship management, just to use one buzz word! If you do work in a company that has been "SAPped", this is a very good resource for you - it should help keeping up with the sort of new developments the IT department like to keep close to their chests!

http://www.nua.ie/

If you're interested in getting some facts and figures and interesting news snippets on ecommerce, this could be a good site for you to look at. It's run by NUA, an internet consulting company who have specialised in surveys and knowledge sharing. You can subscribe to newsletters on subjects of interest to your area. I quite liked making it work which takes a specific sector such as the music industry and asks how it can make the internet work for it. The surveys are also interesting, covering areas like how email boosts productivity for employees (yes really!) etc. Could these be useful statistics I ask myself??

Ecommerce and the law:

http://www.weblaw.org/

Far be it for me to promote the work of lawyers, but, I have to admit that they share with auditors the impression of being a necessary evil. Having said that, this site run by a company of intellectual policy and internet barristers has some useful information on it, in particular sites on the UK Electronic communications bill, the RIP bill Regulation of Investigatory Powers) etc. I found the linked site on trustUK very interesting. TrustUK is a non profit making organisation which has been set up with the support of the UK government "to enable consumers to buy on line with confidence." I had never come across it, but maybe some of you who buy more regularly over the net have, as it has been endorsed by the E-Minister, Patricia Hewitt. This information on laws and policies leads me on to the next couple of sites I reviewed:

The future of Ecommerce:

http://www.savetheweb.org

There has been a lot of noise in the computing press in recent months regarding the new electronic commerce bill, various law suits against service providers for carrying defamatory material, and general comments on issues such as privacy. The Internet grew up unregulated and there have been recent fears as to how much regulation governments will impose. This site firmly sets out its stall against increased bureaucracy on the web and calls on us as users to get involved in resisting laws that might threaten freedom on the web. There is also information on new laws on digital copyright and privacy - the sort of thing that can affect companies whatever industry they may be in.

http://www.oecd.org/subject/e_commerce

This contrasts with this site from the OECD (the organisation for Economic Co-operation and Development) which has its own forum on electronic commerce. From here you can download various documents in acrobat format on areas such as cryptography and authentication to consumer protection and taxation principles. Clicking on the link to the OECD background information brings up another page which points to two other pages on the OECD site which have even more information on this subject. They thoughtfully provide a list of the documents available so you can decide whether to go there. These range from cryptography policies through to telecommunications developments and policy issues.

http://www.itforall.org.uk/aboutit/understandingit/jargonbust.htm

Okay, how many of us have had meetings with very "techie" people who used so many TLAs - oops, sorry - three letter acronyms - and words we didn't understand that we ended up reeling from the information

overload and came away feeling we had learnt nothing? Well I certainly have, so I thought it was worth including this one as my coffee break site for this issue. This particular page contains a jargon busting index which you can search letter by letter for the particular term you require. Could be very useful in that forthcoming technical audit!

Here's a few more tales from the help desk that you may find hard to believe. I hasten to add that they didn't happen to anyone I know…..did they???

An unfailingly polite lady called to ask for help with a Windows installation that had gone terribly wrong.

Customer: "I brought my Windows disks from work to install them on my home computer."

(Training stresses that we are "not the Software Police," so I let the little act of piracy slide.)

Tech Support: "OK. What happened?"
Customer: "As I put each disk in it turns out they weren't initialised."
Tech Support: "Do you remember the message exactly, ma'am?"
Customer: (proudly) "I wrote it down. 'This is not a Macintosh disk. Would you like to initialise it?"
Tech Support: "Er, what happened next?"
Customer: "After they were initialised, all the disks appeared to be blank. And now I brought them back to work, and I can't read them in the A: drive; the PC wants to format them. And this is our only set of Windows disks for the whole office. Did I do something wrong?"

This guy calls in to complain that he gets an "Access Denied" message every time he logs in. It turned out he was typing his username and password in capital letters.
Tech Support: "Ok, let's try once more, but use lower case letters."
Customer: "Uh, I only have capital letters on my keyboard.

INTERNET RESOURCE LIST

AUDIT

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

SECURITY

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

COMPUTER COMPANIES AND SYSTEMS

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

OTHER ORGANISATIONS

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

HACKERS AND VIRUSES

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

AREAS OF AUDIT INTEREST

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

WebTrust, The Net Gains

By Chris Howard

The Internet market place - a dark alley or an international superhighway?

Both consumers and merchants are equally vulnerable to the problems of e-commerce as the expansion of e-business outstrips the ability of management to control that growth. The need is to provide adequate investment in management time and money to ensure websites are safe both in design and operation. There is a clear need for this investment if the Internet is to be prevented from becoming a side alley where only the brave or unknowing would consider venturing for trade.

There are two areas where UK companies are currently exposed. Internet fraud and insufficient supply chain management. A recent survey on Internet fraud carried out by Ernst & Young found that companies were ignoring the dangers which had affected 60 per cent of firms over the past 12 months. The latter problem was starkly exemplified in Christmas 99 with gifts not arriving because management were unable to comply with their own promises regarding terms of trade. If this problem permeated the enthusiastic early adopters, it is certain to intensify once followers with less expertise join the market place.

But the Internet does not need to be like that. What is required is an increased emphasis by business on the development of websites which are safe and secure. There is also a need to educate those who operate them with the knowledge of the risks as well as the benefits of e-commerce. Achieve these and the dark alley becomes a Superhighway on which trade can prosper.

Design the website with security in mind

In any new development, early adopters invest their reputations, their enthusiasm and resources in the adventure. E-traders are no exception and many are doing an excellent job in pioneering the approaches necessary to limit their business risks. However, even amongst these early adopters, the drive for increasing sales through marketing and improvements in direct customer relations takes priority over fundamental elements of the business process. Developing online relationships with vendors, suppliers and partners as well as the security and privacy requirements suffer as a result.

A need for differentiating the good guys from the bad

As the market expands there is a need to define best practice in e-commerce. Only by offering this standard can those businesses operating safe sites be differentiated from others less secure.

WebTrust is a global standard for e-commerce and backed by the Institute of Chartered Accountants who pioneered this standard in the UK. Its principles and criteria create a benchmark against which websites can be compared and monitored. This process involves Chartered Accountants who have undertaken special WebTrust training conducting an independent verification of a website's operations. A 'seal of approval' can then be obtained for display as a badge of quality on the operator's site.

WebTrust's unique facility

But WebTrust provides a further unique facility to the potential e-merchants wishing to develop an e-commerce strategy. By documenting best practice for e-commerce sites to meet the requirements of a Webtrust seal engagement, those same procedures provide guidance on the risks and benefits of e-commerce. By providing e-merchants with the support of trained practitioners in the development of the new site, the risks of trading on the Internet are reduced both for the merchant and the user.

How much does a WebTrust review cost?

The cost of the seal is £900 per annum.

Where merchants use the WebTrust trained practitioners from the earliest stages in the development of their web site, this cost becomes a small addition to the development cost of the site and needs to be compared with the expected benefits from having a secure website whose security and effectiveness has been independently verified.

By assisting management in the development of effective systems and training in the risks and benefits of e-commerce the WebTrust seal review is able to concentrate on the way management have operated and provides a report of adherence to strict principles and criteria appropriate to an effectively managed site.

Continued on page 16

ISACA London Chapter AGM 2000

The Annual General Meeting of the London Chapter of ISACA was convened at the offices of BDO at Baker Street at 4pm on the 18th May 2000 and was attended by about 40 members. In the absence of the Chapter President the meeting was chaired by the Vice President Steve Bailey.

The first item on the agenda was a presentation by the Chapter's Treasurer, Archie Watt, explaining the Chapter's current financial position and the accounts for the year ended 31st December 1999. He pointed out that the Chapter does not exist to make a profit but to provide benefit to the members and that these have been enhanced in the past year with a new improved Datawatch magazine [thanks for that Archie! - Ed] and the welcome return of alcoholic beverages to the monthly meetings which had been well attended - so much so that we were now struggling to find venues big enough to accommodate all the members that wish to come. So if any of you work for companies that would be prepared to host the meetings please let one of the events committee know! Despite these increased benefits we still only aim to hang on to £35 of the subscription fee per member which compares favourably to other chapters in Europe. Talking of other Chapters, the Treasurer pointed out that we have a tie up with the Central and Northern Chapters and that any of you reading this are eligible to attend any of their meetings and vice versa. The other UK Chapters' events are now listed in Datawatch so if you ever are in the appropriate area and have an interest in one of the events of any of the three UK Chapters, you are able to attend. After admitting a closet love of libraries, Archie informed us that the Chapter membership has peaked at 730 and that this obviously increases costs of postage. The Chapter had a surplus of income over expenditure of 5% which was in line with aims and expectations.

Some of the “Audience”

The Secretary Charles Mansour, then read out the President's report for the year, which you can find elsewhere in this edition of Datawatch. He had severe competition from a couple of violent thunderstorms which appeared to have been waiting for him to stand up, though he coped gamely with the distraction.

The next item on the agenda was the elections of Committee members. All were elected unopposed and two new members were welcomed to the committee, Joseph Wright and Michael Christodoulides.

A problem which the committee have recently been experiencing has been that of ensuring that they are quorate at meetings and so can take decisions. The current rules stipulate that 50% plus one is required for a quorum and this has been proving very difficult to achieve. A new suggestion is being put forward and will come out by Mailshot very soon. We'll also have the excitement of an Extraordinary General Meeting some time in the 2000 to 2001 events calendar to look forward to.

At this point the AGM was closed and the audience were all freed to enjoy the excellent refreshments at the back of the room which consisted of beers, wines, soft drinks and a very good range of food too. I can personally recommend the strawberry scones and I think there were a couple of others who were able to recommend the wine after copious sampling! Diet starts on Monday.

We then returned to our seats (some of us with supplies of cakes/drinks etc) to hear our very own Steve Bailey of Steve Bailey Associates present

on the subject of Network Penetration

Steve opened the presentation by stressing the difference between vulnerability testing and penetration testing. Vulnerability testing is looking for known weaknesses in systems, either manually or using automated programs, but it is usually non invasive. Penetration testing on the other hand takes it a step further on, identifying the vulnerabilities and attempting to exploit them. Hence it is invasive and can have serious implications such as causing systems to crash. Steve pointed out that every company should be testing its networks for weaknesses - otherwise it is only a matter of time before this is done by an unauthorised person!!

Steve suggested some points to bear in mind when carrying out this sort of testing. It is important to have in mind why it is being done and what its objectives are.

A harder area to button down is that of policy issues and responsibility for this - it is necessary to have policies in place from senior management but often no one wants to take responsibility or ownership.

There are also legal considerations such as the Computer Misuse Act. It is perfectly acceptable to scan, cause denial of service or break into your own network, but if you do it from an external account, such as one supplied by an ISP you may scan other's networks on the way, especially if you are using a tool such as SATAN. There is also the telecommunications Act to consider which you could easily breach by dialling up to do this sort of testing over a public network.

There are of course financial implications too, such as the time of IT department experts which may be required to rebuild servers at very short notice if your efforts cause them to go down.

Where you position yourself on the network to do these tests is also important as it will determine what you are simulating. If you are testing from the DMZ you may end up testing just the firewall.

It will be helpful to you to have certain pieces of knowledge such as the physical and logical lay out of the system and the software and applications, depending what your test is trying to simulate.

It is helpful to assess what the main threats and vulnerabilities to the system are as this will affect how the testing is done - for example do we see the main threats as being internal rather than external? And very importantly, you will need to back up the systems before you start!

Network vulnerability testing is an iterative process - once the initial vulnerabilities discovered have been addressed the network should be retested. The hackers never stop, so neither can we!

Steve Bailey presenting “Penetration Testing”

10 Years Ago

The following stories show that by 1990 the industry was beginning to take this virus subject seriously.

Internet Worm Man Convicted

A federal jury in Syracuse has convicted Robert Morris of a felony charge for creating and unleashing a disabling computer program. In 1988 some 6,200 computers linked to the federal computer network, Internet, were disabled by his Worm.

Morris faces up to five years in prison and a $250,000 fine. He claimed in court the incident was an experiment that went awry. "I wanted to see if I could write a program that would spread as widely as possible on the Internet," he told the court.

He said he had miscalculated the rate at which the worm would multiply and how fast it would race through the network, when he set it loose on the 2 November 1988.

He is the first person brought to trial under this act, which made it a felony to break into a federal computer network and prevent its authorised use. He could also be ordered to make restitution to those affected by the Worm.

Massive Virus Epidemic?

A US Computer security expert is predicting a massive epidemic of computer virus programs that will infect as many as eight million pcs over the next two years and cause billions of dollars worth of damage, reports 'Computing'.

Peter Tippett, a specialist in computer security issues, has published a paper titled 'Kinetics of Computer Virus Replications'. Tippett uses mathematical and epidemiological tables normally used for predicting the behaviour of biological viruses, to estimate the size of the computer virus problem.

Tippett said the increasing tendency to interconnect PCs was widening the scope of the problem.

Industry analyst Andrew Seybold said: 'I believe the risks incurred from the proliferation of malicious software represent the greatest challenge faced by computer users and professional managers.

EDPAA Datawatch, Vol. 8, AUG 1990

Continued from Page 13 ...

The WebTrust review of existing websites will be costed in the same way as other professional services. The more effective the management controls, the less the potential cost.

What is covered in the review?

The review focuses on security, privacy and delivery. It ensures that the website is free from viruses, that private information is only used for the purposes authorised, and that the supply chain is in place to ensure that goods ordered are received in time and in good condition

The review includes a visit to the offices to confirm management's knowledge and experience of Internet trading, a review of the terms of trade required to be displayed on the Website and the testing of controls and transactions.

Independent verification as a minimum requirement

There are two principal ways of policing the Internet. One is to allow the traders onto the Internet with a seal based on a promise to comply with good practice and wait for complaints from unhappy customers. This is termed passive policing because it relies on reaction to a problem. The alternative is active policing comprising of independent verification of management's knowledge, experience and integrity tested to actual events before the seal is granted in order to reduce the risk of unforeseen or untended, problems. WebTrust adopts an active policing role and engages trained specialists who independently verify the website operations and transactional facility.

There can be no real security in a seal programme which relies on a promise to comply with rules when management may not have the knowledge, experience or internal reporting systems appropriate to an e-commerce operation. Webtrust provides the necessary confidence to site users by verifying that managements' own policies and procedures are being put into practice.

Is the WebTrust service providing a guarantee?

WebTrust provides a guarantee that approved sites are run by quality management. No financial guarantee is given although the website management is required to have appropriate customer redress procedures in operation. WebTrust puts the customer in the same position with a website as he is with a high street store.

The ICAEW Webtrust Seal of Approval is a graphical representation intended to indicate a Website's compliance with the ICAEW Webtrust Principles and Criteria and is reproduced here for illustrative purposes only.

What form does WebTrust approval take?

A seal of approval is affixed to the website. By clicking a cursor on the seal, the WebTrust report, letter of engagement, copy of the WebTrust principles and criteria and other relevant information become available if required creating a transparent record of what has been the nature and the result of the Webtrust review.

The WebTrust seal is itself a secure programme, operated in association with Verisign who act as a certificate authority to activate the seal. Verisign, a leading authority in this field, also has responsibility for checking on all similar seals placed on sites around the world, eliminating those found not to be approved thereby confirming the integrity of the service.

The benefits of signing up to WebTrust

The benefits of e-commerce merchants signing up to WebTrust are two-fold. The first benefits the merchants who, by making an investment in good practice, by incorporating WebTrust into the original business plan, avoid costly mistakes later on.

The second, of more general benefit to the market place, is that incorporation of WebTrust into the design, development and monitoring of e-commerce sites provides a valuable contribution to the safety of the Internet.

It is for this reason that the Institute of Chartered Accounts is supporting this initiative so that confidence in trading on the Internet will increase. If this fails, then the Internet will not release its potential for growth.

The Institute of Chartered Accountants is also working with leading technology companies and Internet providers in developing efficient ways to access e-commerce as well as training projects both of which are targeted at SME's. These developments will be the subject of a subsequent article.

For more information about WebTrust log on to www.icaew-webtrust.co.uk

Chris Howard is the Director of Assurance Services for the ICAEW and is responsible for the development of WebTrust services in the UK. choward@icaew.co.uk or 020-7920-8516

Telephony Security - Corporate Embarrassment

By Duncan McKerracher

In Issue 42 of Datawatch, we outlined the four main issues of telephony security - Toll Fraud, Denial of Service, Corporate Embarrassment and Phone Tapping. In Issue 44 we described Toll Fraud and in future editions of Datawatch we will discuss Denial of Service and Phone Tapping. This article describes an increasingly significant issue, that of Corporate Embarrassment.

Corporate Embarrassment is a very popular type of telephone hacking. Here the hacker usually carries out the work purely for his own amusement. There is sometimes a sinister reason, but in general it is regarded as "a bit of fun". Of course, to the victim there can be potentially very damaging consequences. The financial impact may not be immediate as in the case with Toll Fraud, but the embarrassment and the resultant adverse publicity could potentially cause the competence and integrity of the organisation to be brought into question.

There are three main ways in which corporate embarrassment can be carried out. These are as follows:

Redirection of voice calls

Unauthorised access to the maintenance terminal of the PABX can allow the hacker to redirect inbound calls to inappropriate destinations. Although this is more often used to allow a hacker to make fraudulent calls to effect Toll Fraud, it can also allow the hacker to divert inbound calls (say to the organisations switchboard or call centre) to inappropriate destinations such as adult chat lines or even a competitor. This has a devastating effect on customer confidence.

Changing voice mail or automatic attendant greeting

Where there is insufficient protection of a voice mailbox, the hacker can readily enter that mailbox and change the personal greeting. The effect is that any callers diverted to this mailbox will hear the greeting left by the hacker. In every case this is entirely inappropriate, often being offensive or vulgar in its content. In some cases hackers have been able to alter the greeting of automatic attendants used to front end all inbound calls to an organisation. With the growth the use of automatic attendants, this trend is of particular concern.

Broadcast messages on PA systems connected to PABXs

PA systems are commonly inter-connected to PABXs to reduce the cost of wiring and to increase flexibility (i.e. staff can make PA announcements from any telephone

Example No. 1

TV Broadcasting Company, London

The broadcasting company used an automatic attendant to "front end" callers to one of the company's prime time programmes. The configuration of the automatic attendant was accessed by a telephone hacker using tones generated by a standard telephone handset. This allowed the hacker to change the original greeting to the something less appropriate.

It was more than an hour before it was spotted by which time as many as 5,000 callers had heard this message. The message was promptly changed back to the original, but then the same hacker dialled in again and changed the original message to the sound of farmyard animals. The service was immediately withdrawn.

Although this incident has a light-hearted side, it caused considerable embarrassment for the television company. However, the hacker could have left an obscene or offensive message, in which case the consequences would have been very much more serious.

extension in an organisation.) A poorly configured PABX can allow a hacker to make unauthorised broadcasts on the PA system. Invariably these will be of a rude or abusive nature.

The examples show that Corporate Embarrassment is a real risk to your organisation's security. However, many organisations remain ignorant or unconcerned about this risk. By implementing simple procedures and updating your PABX configuration, it is possible to minimise the risk of Corporate Embarrassment at a comparatively low cost.

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

Example No. 3

Clothing Chain Store, North West

A hacker discovered that by dialling a specific number on the PABX of a large chain store, it was possible to make announcements over the in-store PA system. By dialling in remotely, the hacker was able to make an announcement to the effect that all menswear was being reduced by 50% and that shoppers should immediately make their way to the menswear department. The result was total confusion amongst staff and shoppers alike. The immediate loss of revenue is difficult to quantify, but the embarrassment felt by one of the UK's most prestigious chain stores was immense.

Example No. 2

Recruitment Agency, London

A recruitment agency set up a telephone hotline for people wishing to be considered for a career in a Government Department. This hotline used an automatic attendant to record the caller's name, address and telephone number. Using tones generated by a standard telephone, a hacker managed to change the original greeting. As with the above case, if the hacker had left an obscene or offensive message, the consequences of which could have been very much more serious.

Nevertheless, this incident caused obvious embarrassment to the recruitment agency. The impact on the Government department was even greater as the impression given in the Press was that it was their telephone system that had been hacked. Although this was not the case, its public image was severely tarnished.

SIG News

By Bill Hawkins

The Fraud Prevention SIG is concentrating on e-commerce fraud and has set itself the objective of producing a set of guidelines to be published either as a booklet of as a set of web pages. The group are meeting on a monthly basis with participants drawn from a wide variety of institutions both public and private. The group are identifying the key areas of concern and performing a risk analysis. Meetings take place on the 3rd Tuesday of each month, view the Chapter's web site for details. There is a mailing list for the group, so if you are interested contact John Hunter via mailbox@jhunter.u-net.com.

The SIG concerning Risk is now up and running and for information regarding objectives and schedule for meetings view the Chapter's web site or contact Charles Mansour via: charles.mansour@woolwich.co.uk.

I have been in contact with other Chapters to establish what SIGs they have and I will report more on this in the next issue. However, early indications are that the London Chapter is more advanced in this area than some.

In my last article I mentioned that 'SIGs have a finite life and some have come and gone (e.g. UNIX SIG)'. Well I am now announcing the end of the Network SIG. I have decided to wind up the group as the number of suggestions for presentations was declining, as was attendance. Additionally, information and workshops on network topics are far more prolific now than they were in February 1997 when the group was formed.

The group held fifteen meetings, which have included a wide range of issues, for example, encryption, PBX security, legal aspects of the internet, TCP/IP, structured cabling and firewall security. The group attracted anywhere between 20 and 40 attendees to each meeting and hopefully was successful in raising members' knowledge in a wide range of issues and providing a forum for exchanging views and making contacts. I would like to take this opportunity for thanking all those members (and quite a few non-members) who turned up and took part.

Another success of the group was that presenters contributed articles to Datawatch, indeed two current regular feature columns are the direct result of presentations these being, Internet Security by Deri Jones (NTA Monitor) and Telecommunications Security by Duncan McKerracher. Other notable presenters worthy of mention are Phil Pinder (Pinder Associates) and Professor Fred Piper (London University). A big thank you to all the presenters for their time and effort.

UK-Wide Internet Security Test - Organisations vulnerable to Spam Relaying

By Deri Jones

NTA Monitor are one of Europe's leading Internet Security testers, with more penetration testing customers than an other supplier.

Part of NTA Monitor's activities is to utilise some of the expertise from in-depth customer testing, to perform periodic wide-scale 'real world' Internet security tests in order to highlight security levels in general and to raise awareness among corporate Internet users.

This article explains one such test recently carried out with the single objective of testing for 'Spam Relay' vulnerability. The test was focussed on e-mail serversin the United Kingdom (the '.uk' internet domain). The objective was to cover 99% of the Internet-visible mail servers within the UK, by testing the three "top level" domains:

ac.uk - Academic
co.uk - Commercial
gov.uk - Government

NTA Monitor's tests are 'real world' real data tests, based on probing live systems - they thus provide a far more realistic picture of overall Internet security than 'opinion poll' type surveys. The results of testing are only published as percentages - no "name and shame" lists of organisations found at risk are published.

Previous tests have for example compared the security problems due to the use of software with known security problems across 11 countries of Europe and Japan (November 1998), or at UK governmental systems (April 1999) etc.

The surveys do not involve 'hacking into' or otherwise exploiting Internet systems, instead the surveys run a single, simple test against thousands or millions of live sites. The surveys are carefully designed and implemented and monitored so as to not cause any measurable or noticeable performance on systems - denial of service type tests are never performed.

Spam - what is it and why is it so bad?

Spam - (named for the Monty Python sketch/song about a cafe where there is nothing but spam on the menu) is the sending of large volumes of unsolicited email - typically for commercial gain by the sender (e.g offering a service or product for sale).

No matter that the content, the main issue is that the recipient did not request the mail nor had chance to reject it before it took up their time/effort and PC/Internet-connection resources.

One site that focuses on anti-spam is:
http://spam.abuse.net/others/sites.html

Spam Relaying

Spam Relaying: this is the process where an organisation's Internet email server is configured such that it acts as a middle-man - i.e. it will (i) accept inbound email from outside the organisation that is NOT addressed to the organisation, but to other external organisations, and (ii) deliver such incoming email back out to the targeted recipients.

Why do spammers use 'spam relays'?

Such vulnerable mail servers are often abused by "spammers" to send junk Email - because:

1 they offload the work of delivering the bulk Email: (one email with say a thousand recipients in the TO: line sent from the spammer to the victim mail server will then force the victim server to deliver copies to the thousand separate recipients.

2 they hide the real source of the email - a percentage of spam recipients will be angry and will retaliate by sending email-bombs back, or will report the sending site to their ISP or similar

3 by not sending spam mail from their own servers it prevents them ever being black-listed by the anti-spam lobby

These open relays cause a problem for the Internet community because they make it easier for the "entry level" spammers with throw-away dial-up accounts to send junk mail to large lists.

What's the problem for organisations vulnerable?

An organisation with the vulnerable mail server misued this way, suffers because::

1 the workload of delivering the junk mails can bring the system to it's knees

2 the spam will appear to have originated from the vulnerable mail server resulting in angry Emails, PR damage and possible action from their ISP

3 not only can spammers relay through them, but they can send

spoofed Emails that appear to be sent from staff within the organisation, which are extremely difficult to detect as spoofed.

Test Methodology

The survey determines all the Internet-visible mail servers within each domain. It takes care to only include mail servers that are within the top level domain being tested and also to remove any duplicate mailers. Thus three target lists are built for 'ac.uk', '.co.uk' and for 'gov.uk'

"Spam can and will overwhelm your electronic mail box if it isn't fought. Over time, unless the growth of UCE isn't stopped, it will destroy the usefulness and effectiveness of email as a communication tool"

Campaign Against Unsolicited Commercial Email (CAUCE) (http://www.cauce.org/about/problem.shtml)

A test script then runs as follows, once for each of the lists. A test message is sent to each mailer, which is addressed from one Internet mail address to another Internet mail address. The test message contains a unique cryptographic signature, which is used later, see below.

As both the "From" and destination "To" addresses as well as the source IP address used are all outside the tested mails server's domain, it should not relay the mail. If it does and the Email arrives at the destination then the mail server is vulnerable to the open relay issue.

(To be totally sure that the email received is indeed the one sent, the unique cryptographic signature mentioned above is checked to ensure it's the same as was sent to that server. This is to prevent the scenario where an eagle-eyed systems admin staff member sees the test message, and tries to upset the survey findings by creating hundreds/thousands of fake emails, from many domains, each a copy of the email sent to them; to make it appear falsely that many systems were vulnerable).

Definition of "Email servers"

The Email servers shown in the results tables represent unique Email servers, not individual domains (there are many more individual domains than unique mail servers). Many domains use the same Email server and we were careful to "de dupe" the mail servers both by name and also by IP address to ensure that each mail server was only tested once.

We were also careful to only include those mail servers that belong within the domain being tested. This means that only mail servers run within the gov.uk domain are included in the gov.uk results and mail servers run by ISPs or commercial or academic organisations on behalf of gov.uk domains are not included.

Results

Domain	Servers Tried	Servers Vulnerable	% Vulnerable
ac.uk	776	166	21.39
co.uk	14,868	4,139	27.83
gov.uk	310	117	37.74
Total	15,954	4,422	27.71

Definition of "Servers Tried"

The Email servers tried column represents those mail servers which we were able to successfully connect to and complete an SMTP transaction (whether that transaction was accepted or rejected). This means that we've excluded those mail servers which were down or which didn't respond quickly enough.

Government GSI connected organisations

"Spamming is the scourge of electronic-mail and newsgroups on the Internet. It can seriously interfere with the operation of public services, to say nothing of the effect it may have on any individual's e-mail mail system. ... Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorization."

Vint Cerf, Senior Vice President, MCI and acknowledged "Father of the Internet" (http://www.cauce.org/about/problem.shtml)

"The MAPS (Mail Abuse Prevention System) RBL (Realtime Blackhole List) is a list of networks which are known to be friendly, or at least neutral, to spammers who use these networks either to originate or relay spam. As we discover such networks, we deny them access to the part of the Internet that we are paying for. Because our research into the attitudes and policies of network owners is hard to duplicate, many dozens of other network owners have asked for and are now receiving a real time mirror of our MAPS RBL.

"Irrespective of the laws of whatever land a spammer, or a spam victim, is in, we consider spam to be theft of service. Internet users do not pay their access fees for the purpose of being annoyed. None of us bought our computers or modems for he use of so-called advertisers...."
Paul Vixie - MAPS (www.mail-abuse.com)

This survey only covers Internet-connected mail servers. Thus mail servers fully inside an organisation are not covered.

This means that individual Government organisations that connect to the Government Secure Intranet (GSI), rather than directly to the Internet, won't be tested, although those with a direct Internet connection will. Nevertheless, the Internet email gateway for GSI sites will itself be tested.

This means that the "gov.uk" results will consist of local government plus those central government departments and all other .gov.uk domains with direct Internet connections.

Our summary of the findings:

We found the figures in general to be much higher than expected. This spam relaying problem has been known for several years now and just about all modern mailers address this vulnerability (although some require manual configuration to do so). Most, if not all, UK ISPs have addressed this problem on their own mail servers. Based on our experience through our "Regular Monitor" penetration testing service, we would have expected a figure of

around 10%. Perhaps this indicates that the people who take our testing service are already aware of the security issues and are therefore less vulnerable than the average.

What does a company need to do to protect itself?

Generally, it's a no-cost solution - virtually all email software less than 2 years old can be configured to not be spam-vulnerable. You need to configure the system so that it knows which mail domains belong to the organisation, and then it can easily reject mail intended for anywhere else.

The comparative results of Government being the worst followed by Commercial followed by Academic was expected. Our explanation for this is:

- Academic institutions tend to configure their mail servers well - this doesn't require new software or cost money, just time and experience. However, our testing did not look to see if organisations are running more email servers for their sub-domains (eg usersx@london.company.com & usersx@newyork.company.com - for a two-office organisation). Thus it is possible that in academic institutions (where individual departments take control of their own email servers) there may well be less-secure servers spread around the departments.

- Government organisations often run older mail systems - often because of security 'ITsec' certification requirements - and tend to make changes less often. Many of these older mailers, and indeed old versions of certified firewalls, do not address the "open relay" issue.

NTA Monitor
www.nta-monitor.com

Note: Security Issues and the computer misuse act

All of NTA Monitor's widespread Internet test surveys are carefully planned and implemented so that they do not fall foul. The tests do not involve exploiting any security holes that are found, and involve the sending of carefully constructed normal and abnormal internet traffic in such a way that it will have zero impact on the receiving system. In this current survey, the test involved the sending of at most one email to each server - the load to an email server of handling one single email are minute. The email was addressed to a third party user and not a user at the target site. Thus no staff or users at the target sites would have received a spam email. Sites where the mail systems were configured OK to block spam relay would have rejected the email, which would have showed probably as a single line in the email server logs.

To prevent the data falling into the wrong hands. as soon as the test data has been compiled into percentages for each type of domain (.ac/.co/.co.uk), the raw interim test result files are then deleted. Copies of the data for any one or more organisation are not kept, only the percentages.

CISA for the New Millennium ... *continued from page 9*

5. Business Application Systems Development, Acquisition, Implementation & Maintenance - Evaluate the methodology and processes by which the business application systems development, acquisition, implementation and maintenance are undertaken to ensure they meet the organisation's business objectives.

6. Business Process Evaluation & Risk Management - Evaluate business systems and processes to ensure that risks are managed in accordance with the organisation's business objectives.

7. The IS Audit Process - Conduct IS Audits in accordance with generally accepted IS Audit standards and guidelines to ensure that the organisations information technology and business systems are adequately controlled, monitored and assessed.

When they are all formally released by ISACA, the actual wording of the above may change as these should be regarded as our first draft, but objectives and implications of subject matter are as shown.

Domain 7, the only "process based" domain, is virtually the old Domain 1, but more directly related to the work of the IS Auditor. In terms of the structure of the examination, the Board has used the statistical analysis of questionnaires to produce the following weighting of questions in the exam:

· Domain 1 = 11% (22 questions)
· Domain 2 = 13% (26 questions)
· Domain 3 = 25% (50 questions)
· Domain 4 = 10% (20 questions)
· Domain 5 = 16% (32 questions)
· Domain 6 = 15% (30 questions) and
· Domain 7 = 10% (20 questions)

The 2001 CISA Revision Manual

We are already in the process of writing a new CISA manual for the restructured examination, and fairly well advanced too. I have already reviewed the first draft of the chapters on Domains 3 and 4, security and continuity being my particular subjects, professionally speaking.

Meanwhile, the Certification Board meet again in June to look at a few hundred exam questions, new ones from Item Writers as recommended by the TEC; new ones we've written ourselves to fill some of the gaps; old ones that really need to be reviewed and updated and quite a few that fall into more than one "domain" so need to be allocated into a "primary" and "secondary".

I hope you'll see that ISACA, and the Certification Board in particular, are working very hard to make sure that the CISA designation is, and will continue to be, the highly respected, truly international qualification it is today.

The Security Column

By John Hunter

I used to think that it was getting harder to keep up to date with the mass of information about technical vulnerabilities that our systems are open to.

Every month the volume coming in seems to get bigger and bigger. I'm now having a bit of a change of heart on this - perhaps it just that there are more people openly on the lookout and sharing what they find. A few years ago it seemed that there were only a few specialists manning the fort and many vulnerabilities were (my Word grammar check tells me that this should be 'much vulnerability was') technically difficult for ordinary users to understand. So much so that Microsoft and other software houses' reporting of them on their web sites was an open invitation to hackers who could afford the time to experiment. After all, they only wanted one to work, whereas we had to understand all of them. These 'bug reports' were supposed to be publicised so that users could keep their systems fairly up-to-date. The trouble was that without interpreters to explain the jargon, many system administrators didn't know which, if any of the problems applied to them - so ignored them. There is now also a problem of quantity, many flaws are not corrected because the administrators simply do not know which of over 500 potential problems are the ones that are most dangerous, and they don't have the resources to correct them all.

Thankfully the situation is improving and there are many excellent information sources available. One that I want to bring to your attention (as it has an element of practical risk analysis) is SANS Institute's web page: "How To Eliminate the Ten Most Critical Internet Security Threats".

This is a listing of experts' consensus on the subject. I recommend you read the information and, even if you do nothing else, check that your site is secure against the ones listed. The site is dynamic and regularly updated. It includes step-by-step instructions and pointers for correcting the flaws and they say that they will update these instructions as more current or convenient methods are identified. Also in the document there is a list of the ports used by commonly probed and attacked services. By blocking traffic to those ports at the firewall or other network perimeter protection device, you can add an extra layer of defence to help protect against configuration mistakes.

SANS say that the majority of successful attacks are the result of only a few software vulnerabilities because attackers are opportunistic - taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely available attack tools. They count on organisations not fixing the problems and they often attack indiscriminately, for example by scanning the Internet for vulnerable systems.

The list is certainly a great example of active co-operation among industry, government, and academia. A lot of participants contribute information including many high profile federal agencies, security software vendors and consulting firms.

The list can be found at http://www.sans.org/topten.htm

And now for a little nag. I regularly receive email 'circulars' from friends and business colleagues. You know the sort of thing - they have received a neat bit of information that they must pass on to their contact list. So they pass it on, with everyone's email address either on the 'To:' or on the 'Copy:' lines. Even worse, the message body often isn't cleaned up and so has a long list of email addresses from the person who forwarded the snippet to him. What happened to privacy? Email addresses given in confidence etc - exponentially spread - doesn't seem right somehow… There's also the Commercial aspect. Presumably everyone gets to know the previous senders list of contacts. I know I've been sent quite a few private lists of contacts this way. If you want to avoid the problem, just use the blind copy ('Bcc:') box for your recipient list and please don't just forward what you receive, do spend some time cleaning it up.

I.T. Auditing and Banking

By Adrian Simpson BSc ACA FIIA

The recruitment market for bank I.T. auditors is without doubt large and influential but curiously compacted into a small geographic area in the City of London.

In spite of this, the roles undertaken by I.T. auditors working within banking vary significantly.

Banks, whether global investment banks or familiar high street names, are amongst the largest and most sophisticated users of I.T. It is not unusual in an investment bank to find that I.T. staff account for as many as 25% of the total headcount, whilst the I.T. budgets of the clearers exceed the profitability of many FTSE 100 companies.

The I.T. risks associated with banking however, are by no means confined to the obvious stereotype of hacking into money transmission systems such as SWIFT. I.T. resiliency and availability currently represent the number one issue within the banking community. Consequently, a considerable amount of I.T. audit resource is now focused on this area. I.T. within banking is all pervasive, from customer facing systems, to back office applications, to general ledgers and risk management systems. The reputational issues associated with an inability to deliver a satisfactory service are clear, especially in light of the adverse publicity associated with the banks recent decision to migrate away from traditional, human resource based delivery channels such as branches and sales forces to electronic solutions such as the internet.

A key feature of I.T. audit in banking is the range and diversity of environments. Large IBM and Unisys mainframes continue to feature heavily in the clearing banks where large volume transaction processing still dominates. Many still run applications developed 30 years ago in Assembler and COBOL. Alongside such legacy environments, vast client server configurations now exist together with fault tolerant Tandem machines and DEC and IBM mini-computers. The demand for technically skilled auditors, fully competent in installation reviews of operating systems and networks is still a core requirement of bank I.T. auditors. Smaller banks together with the investment banks have a heavy concentration of client server computing, NT and the ever present Unix platforms.

I.T. audit work in banking also focuses on traditional application reviews in support of operational audits together with ever critical system development and project management reviews.

Another feature of I.T. audit in banking is the exposure to high profile leading edge technology, currently the brave new world of e-commerce. In practice it has been the banking community which has been at the forefront of many of the more substantial developments in this field, pushing back the barriers of technology, political ignorance and the legal framework. The ability to perform internet banking or share dealing by WAP phone would have been unthinkable only 18 months ago but is now regarded as being a core service. The whole debate on public key encryption has been escalated and accelerated as banks pursue the need to have affordable and effective encryption.

The change imposed as a result of e-commerce has been both substantial and rapid. Many of the risks associated with this area are only now being discovered and not surprisingly, the audit approach is still evolving. The need for creativity and flexibility are now prime requirements of any bank I.T. auditor.

Despite a turbulent period of rationalization and merger activity, the demand for experienced I.T. auditors remains strong. Whilst a premium is available for relevant banking experience, I.T. audit experience is proving marketable to other areas within banking such as project management, I.T. security and operational risk. Bank auditors are increasingly being lost to these areas. This offers opportunities to non-bank auditors who are well qualified or possess strong technical skills, particularly in areas such as Windows NT, UNIX or e-commerce.

The majority of vacancies are for experienced bank I.T. auditors who require little supervision but are not yet aspiring to management. Banks are generally not keen to train I.T. auditors and prefer to buy in appropriate skills. This has tended to contribute to salary inflation in banking. However, higher salaries have to be justified and I.T. auditors cannot expect a significant salary leap just because they have joined a bank. I.T auditors in the City very often work longer hours and the environment can be pressured.

The current trend towards specialists within banking is also worth considering. Whilst smaller banks employing only one or two I.T. auditors have generalist I.T. audit roles, in larger banks, I.T. auditors are more likely to concentrate exclusively on one area such as applications, developments or infrastructure. This type of specialisation can be frustrating.

New technology is forcing developments in I.T. auditing and nowhere more rapidly than in banking.

Central News

By Michael Hughes, President, Central UK Chapter

Well its AGM time again and therefore we are nearly half way through the year already ! It only seems five minutes ago when the merchants of doom were predicting the end of the world as we know it. Well we are all still here.

On the subject of the AGM, the new committee was elected to their year of service, so please make sure you look towards the front of Datawatch for the new line up. There aren't too many changes, we have had one resignation, Melanie Ogden has moved on to bigger and better things at IBM which has resulted in her moving away from the central region, so I would like to take this opportunity to thank her for all her hard work on the committee and wish her good luck in her new role. I would also like to thank Ken Perry for volunteering (I think that's the correct term, Ken may have other views) and welcome him to the committee.

The Chapter has now been running for six years and in that time we have seen the membership grow from 25 to 126 today. Whilst we still want to grow the membership, we also want to encourage more members to come to our evening meetings. We generally get between 25 - 35 members coming along to these meetings, and we generally receive good feedback from attendees on the guest speaker and the content of their talk. It also gives members the opportunity to get a bite to eat, drink and speak to colleagues in other organisations, who may have already solved the problem they are currently wrestling with. We are about to canvass members views on the kind of events you want, so please take some time to complete the questionnaire and send it back. In the good traditions of the Readers Digest, all returned forms will be entered into a prize draw for a £50 gift voucher. So come on, this is your chance to have your say and let us know the sort of events you want your committee to organise. On the subject of events, please note the change of dates for our last two events of the season. On behalf of the committee, I apologise for the changes which were outside of our control. The best source for up to date information on our events can be found on the Chapter's web site: www.isaca.org.uk/central.

Whilst I'm on the subject of giving away money, can I remind members of the two bursaries which we operate. Members of the Central Chapter can claim £50 for either a CISA question they write and get accepted for inclusion in the exam, or for a article they write and get published in either Datawatch or the International Journal.

With Chapter business out of the way, I'll turn to more day to day issues such as what issues we IT risk professionals should be focusing our attention on?

How about IT governance?

International HQ are starting to promote this issue and have recently set up a web site dedicated to the subject, which is well worth a visit, www.itgovernance.org.

But why is IT Governance becoming such an issue ?

Information systems are becoming more complex and deeply integrated in the core business processes of an organisation and at the same time there are pressures to reduce cost. Information Technology, long considered solely as an enabler of an organisations strategy is now regarded as an integral part of that strategy. Senior management are waking up to the fact that strategic alignment between IT and business objectives is a critical success factor. IT Governance helps ensure achievement of this critical success factor by efficiently and effectively deploying secure, reliable information and applied technology.

In the wider context of Corporate Governance, here in the UK we have the Turnbull Committee report (available to download with Acrobat reader from: www.icaew.co.uk/internalcontrol/).

Organisations can view Turnbull in two ways: as another layer of bureaucracy that can be followed to the letter but not in sprit; or as a means of adding value. I believe, if implemented in the right way, that Turnbull can add value as it

encourages organisations to embed good risk management into everything they do. This should make them more flexible and able to respond more quickly to both manage threats and to fully exploit opportunities.

In many cases, the process for identifying, reviewing and disclosing risks will be highly dependent on IT systems. When reviewing the effectiveness of the system of internal control (as compliance with the combined code and Turnbull requires), the board will inevitably have to consider whether their IT systems are helping to report risks in the right way and whether they are sufficiently robust. But does the board really have the depth of understanding necessary to challenge these issues ? In my experience, even sophisticated organisations often lack the sort of measures needed to track IT risks. IT systems are a vital part of the business, the board must have an appropriate IT governance structure in place to ensure that the organisation:

- ✦ effectively addresses business issues such as Year 2000, e-commerce, ERP etc;
- ✦ maintains the security, reliability and integrity of the organisations strategic information;
- ✦ protects the organisation's investment in information systems and IT infrastructure;
- ✦ ensures the appropriate management of the organisations information assets.

So what should IT risk professionals should be doing ?

We all have a challenge to bring IT governance issues to the 'top table', it took some considerable time before many boards woke up to the potential damage the Year 2000 issue could impact on their business. This highlighted the lack of boardroom and organisational wide awareness of IT risk. With so many organisations dependent on their IT systems for day to day operations, the impact on a simple e-mail virus such as the 'I Love You' or 'Melissa' viruses can be enormous.

Organisations need to consider how business risk is being identified and managed for both good business management and to comply with the Turnbull report.

Who's considering IT governance issues ? Who if not you ??

Central Chapter Programme of Events

22 September 2000
Business Continuity Planning

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

Northern News

By Ray Butler

I'm writing this in the week after a really great pair of two-day Professional Seminar Series events on Internet Control issues & audit methods, delivered by Don Caniglia. As well as the learning, it gave the chapter committee the chance to meet a whole lot of members & potential members from all over, and to show ISACA's technical leadership off to the world (or at least our corner of it.)

I'm also writing three weeks before our AGM - by the time you get to read this the chapter contacts in the front of Datawatch will be out of date. I'm very glad to say that a number of new volunteers have come forward for election to the committee, and very sorry indeed to say farewell to two officers: Gillian Peschke, who's done a great job in the vital, but unsung, job of treasurer for the past year, and Lynn Lawton, our past the North for many years. Thanks is an inadequate word, but it'll have to do.

Soapbox (or perhaps a pile of COBIT v.1 boxes)

The chapter has also had an excellent presentation from Vernon Poole, a founder member of the chapter and a member of the IT Governance Institute's board - The Institute is a really exciting development for IS auditors, and we all need to nurture it. Why ? Well, in the same way that you can't be any sort of an auditor without being some sort of Computer Auditor, you can't have good corporate governance without having sound IT governance.

This will obviously bring the benefits of IS audit right to the top of the corporate "in" tray, but Vernon and his colleagues are not fairy godparents waiting to shower benefits on us. We've got to take stock of what IT audit is for, and to play our part in developing our organisations and adding value. Old news perhaps, but there are still those out there who think that auditors come onto the field of battle to bayonet the wounded.

We mustn't feel threatened by the spread of what was IT auditing into the mainstream - things like CAAT tools becoming end-user computing, the emergence of IT security as a profession in its own right. The role of the IT auditor may be changing - from auditing in the traditional sense to facilitating audit, control and governance by others. We can lead this by bridging the gap between business technology and business governance, but to do this we must speak in pounds and assurance, not bits and bytes. The traditional image of the auditor is someone who goes looking for problems to complain about. The future is in looking for solutions to celebrate - and if the IT governance institute delivers what it promises, that future is a rosy one.

NEWSROUND

By "The Newshound"

IT Security stuck in the Past

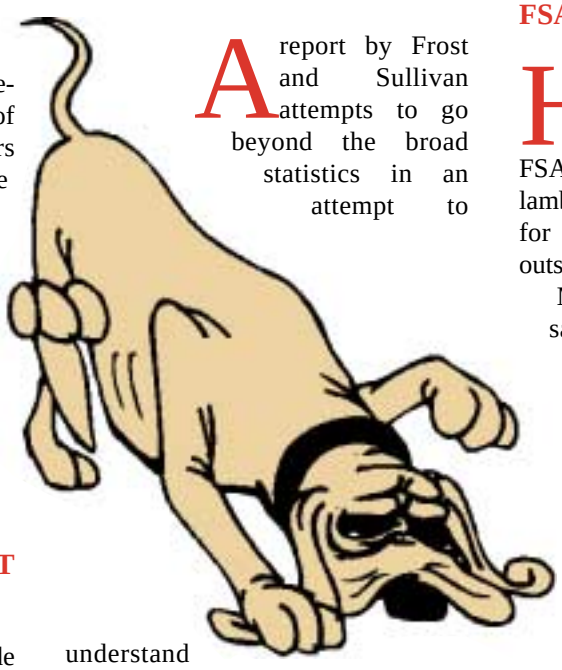
IT Security specialists OVUM have rounded on UK IT Directors for poor security practices. OVUM analyst Graham Titteringham has accused UK companies of relying upon outmoded security practices which rely upon *"preventing users from accessing networks as opposed to protecting confidential information once the user had gained access"*. Titteringham went on to add that *"the biggest threat to corporate networks lurks within the boundaries of organisations"*. Companies which are able to demonstrate sound security practices in the era of e-commerce, would gain the trust of customers and business partners enabling them to leverage core business opportunities.

A major drawback for companies in the current environment is the lack of interoperability capabilities among vendors, which prevents the implementation of integrated security management systems which co-odinates security tools with applications.

DTI finds 'sub standard' IT Security in UK companies

In April the Department of Trade and Industry unveiled the results of survey into IT Security in UK companies. The report makes salutary reading, revealing that over 80% of companies with external links through the Internet have no firewall protection and over 50% have no WEB site security. However, the threat from computer viruses appears to have penetrated senior management psyche with 83% having implemented virus protection and password controls, (the report does not reveal how many organisations maintain the currency of their virus detection software however!). E-Commerce Minister Patricia Hewitt stated at the launch of the report that *"Information security is about guarding your business' money, image, reputation and potential. The consequences of security incidents can be disastrous but they are avoidable."*

Fear and Cynicism in the Boardroom



A report by Frost and Sullivan attempts to go beyond the broad statistics in an attempt to understand why IT security in many UK companies is so abysmally poor. The report concludes that talk of security in business circles inevitably conjures up the twin emotions of fear and cynicism among the denizens of the Boardroom. Fear drives the purchase of security devices such as firewalls but cynicism inevitably creeps in when successive waves of salesman try to persuade organisations to part with ever increasing quantities of cash to protect the organisation from another devilish but unidentified 'cyberfoe'. According to Frost and Sullivan this helps to explain why *"a whole raft of IT administrators don't consider extra investment in Internet security products as justified."* This ambivalence, argue the authors, is also related to the complexity of many of the products on offer which fail to make the connection between the security problem they solve and the needs of the business. This makes businesses reluctant to push ever-increasing quantities of money into a 'black hole' labelled IT security for they see little obvious benefit. Sadly, the only occasions on which this mind set is actively challenged is when a tangible security problem reveals itself and proves to have a business impact. By then of course, it is usually too late.

FSA Wake-Up call to the Banks

Hot on the heels of the Cruickshank Report and the row over ATM charges, the FSA has waded into the fray again, lambasting financial services firms for not taking enough care when outsourcing IT functions.

Michael Foot, head of the FSA, said financial companies' senior managers are not aware of ongoing IT projects, and that they are failing to take responsibility when IT projects go wrong. He also said that finance companies are cutting costs by not employing enough staff to work together with the contractors.

Gary Cooper, research manager at analysts Butler Group, blames mis-communication between outsourcing companies and their customers. Cooper said: *"In large corporations, the IT decisions are made without consulting the relevant IT managers working with the project itself. IT managers need to be involved in the decision making at all times, not just when it comes to the execution of the project". "When IT projects go wrong, the management*

starts to look for someone to blame. Cost effectiveness to a financial company will become short term if the project fails because of poor communication between departments." he added. But Paul Bradford, head of corporate IT at Prudential, claimed his company has adopted a more responsible approach. *"At Prudential, each business unit makes a decision independently and any IT related issues will go through the IT department. If we have a service level agreement (SLA) with an outsourcing company, it is up to the sector manager to follow that particular arrangement."* he said.

Anti-Virus Companies call for a 'Most Wanted' List

Europe's leading anti-virus companies are calling for the establishment of a unified virus grading system to prevent the media from spreading hype and misinformation about new attacks.

According to security experts, the media is to blame for creating unnecessary panic after the FBI posted an alert about the 'Resume - Janet Simmons' virus during May bank holiday weekend. Kevin Street, technical manager at Symantec, wants to see an independent, centralised organisation controlling the dissemination of security information. He said: *"A vendor-independent body should be in place which weeds out the true hazards from minor viruses. A subscription-based grading system would allow companies and the media to access a global system whereby threats could be made scalable."*

Mikko Hypponen, manager of anti-virus research at Finnish security company F-Secure, blames in-fighting between vendors for the lack of unified alerts. According to Hypponen, open communication between virus experts is not always practical for reasons of competition. *"Security companies are too protective over new virus alerts as they want to be the first ones to provide their customers with protection from the attackers."*

Dave Ball, European vice president of marketing at Computer Associates, praised the media for raising awareness. He said: *"Any attention to corporate security issues is important."* But Graham Cluley, senior technology consultant at Sophos claimed the media has acted irresponsibly in the past. *"There are some in the media who find it very easy to just take what the anti-virus vendor has said on face value, rather than seeking other opinions about the size of a threat."* he said.

Amazon declares an end to the Goldrush

For those of you who invested in '.com' stocks it will come as no surprise that Joe Galli, the Chief Operating Officer of Amazon.com has officially declared the race to carve out a niche on the Web by collecting customers at a loss is officially over. Galli is predicting a new era of consolidation with the dominant players in each market sector now established and unlikely to be ousted. He stated that Amazon would not have been able to start-up in the current business environment and the approach of the company would need to be radically different. Galli does not believe that the recent fall in Internet stocks has harmed Amazon in fact he feels that company has gained from a maturing market place, *"Six months ago we had new competitors starting every day. Now investors are more discerning and they realise it is impossible to usurp the established online brands."* Dr Patrick Forth, Vice President of the Boston Consulting Group agrees with the comments, *"In the book written about the Internet, chapter one has now been written and it was about 'land grab'. We are now back to traditional economics."* The comments were also reinforced by Olivier Beauvillain, analyst at Jupiter Communications, *"There is definitely still a place for traditional bricks and mortar retailers to get into the market, but for new Internet-only start-ups, the game is largely over, especially in the US."*

Snooping Bill faces a Battering

At the time of writing the so called 'Snooping Bill', the The Regulation of Investigatory Powers (RIP) is facing close scrutiny as it enters committee stage in the House of Lords. This is one of the final opportunities for any substantial changes to be made to the 74-clause Bill which gives law enforcement agencies greater powers to intercept Internet communications.

A total of 229 amendments have been tabled. The most significant of these - as proposed by Lord Cope - would improve the position of Internet Service Providers (ISPs), as it makes provision for the creation of a technical board to approve any interception. Another proposal suggests the government pay for the bulk of the compliance costs.

Roland Perry, director of legal affairs at London Internet Exchange (Linx), said: *"I am pleased about Lord Cope's call to set up an approval board, which the security services can go to for guidance on what sort of interceptions are feasible. This board will be able to disallow notices that just aren't possible to comply with."*

More limited changes are likely to be made in the most controversial part of the Bill - clause 49 - that reverses the burden of proof if a person holding an encryption key can't disclose it for any reason. The amendment would also limit the amount of time that a key holder will be held liable under the law.

This could be particularly important for businesses where the person responsible for holding the key leaves the company. However, Lord John Cope, leader of the opposition to the Bill in the House of Lords, was doubtful that many of the amendments will be passed. *"It is easy to find opposition to the Bill, however what will be harder is to get enough agreement on the necessary remedy to actually pass an amendment."* he said.

Caspar Bowden, director at the Foundation for Information Policy Research (FIPR), argued that the amendments are simply "window

dressing". He said: *"We've seen a rise in opposition but there is still no sign that the government is prepared to back down."*

Snooping Bill: LSE and the British Chamber of Commerce launch attack

The British Chamber of Commerce (BCC) and the London School of Economics (LSE) released a report in May highlighting new evidence of the damage the Regulation of Investigatory Powers (RIP) Bill will have on British e-commerce.

Chris Humphries, director general of the BCC, stated that his institution and the LSE commissioned the report to prove the Bill is a serious threat to British business. The report came as the House of Lords was preparing to meet for to debate the issue. He said: *"We can now produce real evidence to the House of Lords of what the general implications of the Bill on businesses will be, and why they should challenge the wording in the Bill to protect our ability to compete effectively on the global stage."* Humphries criticised the proposed legislation in an open letter to the Home Secretary saying it represented a serious invasion of commercial privacy. His response was supported in a statement released by the Institute of Directors (IoD).

Jim Norton, director of e-policy at the IoD, echoed Humphries' earlier criticism that the Bill could stunt growth of British ecommerce. Norton said: *"The UK stance on this Bill is worrying many companies - especially multinationals who contrast the proposed UK legislation against far more business-friendly proposals in Ireland, France and Germany and even the USA."*

Governments 3G Bonanza slammed by Expert

Internet guru, Nicholas Negroponte, has accused the UK government of mortgaging its future by pricing third generation (3G) mobile technology out of the range of most consumers. Negroponte - an MIT professor and author of zeitgeist prediction 'Being Digital' - said countries all over the world envy the UK Treasury's £22.5bn windfall. However, he argued that with a base cost of approximately £1,000 per user, 3G technology is now economically untenable and out of the reach of average consumers.

He said: *"I cannot tell you how disastrous that auction was, in terms of the impact it will have on the Internet and consumers. France and Germany want to do the same. Spain and Scandinavia - who gave it away for free - are kicking themselves. It sets a precedent that is truly not economically supportable."*

The people who arranged the auction are not 'digital', he added, and now they'll force the nation's young people to live without the latest digital services. Negroponte said that with British consumers unable to afford 3G, they will rely on lesser technologies like GPRS (General Packet Radio Service) instead, possibly making the investment of the licence holders pointless.

UK e-envoy Alex Allen dismissed the claims. He said the high cost will mean competitive pressure on licence holders to roll out services quickly. Allen added: *"The £23bn will be used to reduce the government debt and that will help the economy. That will mean a saving forever of £5bn per year."* Negroponte was speaking at an ihavemoved.com event.

UK government to end Public sector IT disasters

The UK e-government minister, Ian McCartney, has issued a damning criticism of the government's performance on IT projects - and pledged that past mistakes will not be repeated. His criticisms came at the launch of a Cabinet Office report, entitled Successful IT: Modernising Government in Action, which lists 30 recommendations designed to avoid the IT disasters that have plagued the public sector in the past.

McCartney promised radical changes to the system by which IT projects are conceived, tendered and implemented. He said: *"There's been no clarity about the ownership of the objectives, no clarity about who was responsible for the management of the project, no clarity or sense of a system in place to deal with risk management."*

The report calls for every project to be assigned a senior official who will oversee it from concept to completion, and for large IT contracts to be broken down into more manageable component parts.

David Davis MP, chairman of the public accounts committee, welcomed the report. He said in a statement: "Making these changes happen is key, and I am particularly glad that in future senior civil servants will be clearly accountable for the extent to which they have applied the guidance."

Peter Gershon, CEO of the newly-formed Office of Government Commerce (OGC), said the changes should help departments make better choices about IT suppliers.

Gershon said: "In the past, there was no mechanism by which government could see how a supplier is performing on a range of different contracts." Such information will now be held in the OGC, giving departments the ability to compare a supplier's record with other public sector clients.

Answers to Linkages on page 2 ...

1. Match
2. Road
3. Cut
4. Son
5. Boot
6. Easy
7. Train
8. Ink
9. Over
10. Imp

The initial letters of these answers form the word "Biometrics"