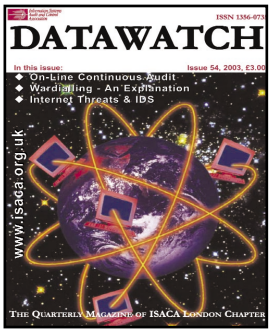
Issue 54, 2003

DATAWATCH

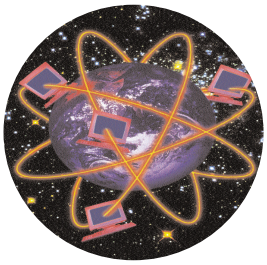


Information Systems Audit and Control Association

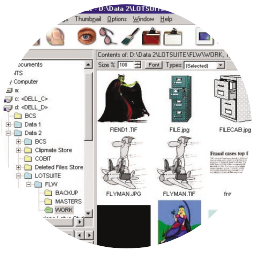
DATAWATCH is published by the ISACA London Chapter. Membership of the chapter entitles one to receive an annual subscription to DATAWATCH.

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

In this issue:



regulars



ISACA London Chapter Committee 2002/2003

President
Charles Mansour

01322-223714
cmanso@globalnet.co.uk

V.P./Webmaster
Allan Boardman
Goldman Sachs
07881 930914
allan@internetworking4u.co.uk

Treasurer
Archie Watt
BDO Stoy Hayward
020 7893 2671
Archie.Watt@bdo.co.uk

Secretary
Joseph Wright
HSBC Holdings PLC
020 7260 6843
Joewright@HSBC.com

Past President
John Mitchell
LHS Business Control
01707 851454
john@lhscontrol.com

Publications
John Hunter
HLB Development Consulting
01635 248944
jhunter@hlbdc.com

Publications
Paul Fortmann

07799 714267
paul.fortmann@btinternet.com

Publications/Research
Kamal Khan
Rabobank International
020 7809 3935
khank@rabo-bank.com

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

Membership
Terry Fallon

01189 473511
Terry.Fallon@talk21.com

Events
Nick Fellows
Barclays Bank plc
07775 543153
nick.fellows@barclays.co.uk

Events
Peter Andrews
PJA Consulting Ltd
020 8540-0224
pa@pjaconsulting.co.uk

Events
Mark Hughes
London City Audit Consortium
020 8836 5899
mark.hughes@bartsandthelondon.nhs.uk

General
Christine Maxwell
KPMG
020 7311 2327
christine.maxwell@kpmg.co.u

General
KevinHandscombe
KPMG
020 7694 6083
kevin.handscombe@kpmg.co.u

Chapter Office
Nancy Watt

01487 814168
nancy@isaca.org.uk

ISACA Northern UK Committee (officers only)

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

Vice President
Robert Newbould
Corus plc

Bob.Newbould@corusgroup.com

Treasurer
Ian Simpson
Halifax plc

IanDSimpson@halifax.co.uk

Secretary
Peter Thompson
Deloitte & Touche

peter.thompson@deloitte.co.uk

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

CISA Co-ordinator
Gan Subramaniam
Homeloan Management Ltd
01756 692147
gsubramaniam@skipton.co.uk

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

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

ISACA Central UK Committee (officers only)

President
Mike Hughes
KPMG
0121 232 3207

Vice President/CISA
Simon Parker
Capital One
0115 843 6456

Secretary
Chris Chandler
Arthur Andersen
0121 233 2101

Treasurer
Geoff Adey
KPMG
0121 232 3202

Past President
James Whittaker
BT
0121 230 2214

Website:

www.isaca.org.uk/central

This month's articles come from a variety of areas among all the regular items you may have come to expect.

Kevin Handscombe's article on continuous auditing is refreshingly practical after the mostly academic articles I have recently read. If you found Dr Neil Barrett's presentation at December's chapter meeting informative, don't miss his follow up article on IDS (that is Intrusion Detection Systems and not the political leader). Following along the lines of communication security, the short article on war dialling has some guidelines for the beginner and some reminders to those who have done it before. Companies wanting my mother's maiden name for security have always amused me. It's a complicated foreign one that I suppose is an advantage over a common more easily guessable one. However, because of that, everyone keeps asking me to spell it, which I frankly can never do that same way twice. So it always comes down to my postcode and date of birth! It is good to see Brian Shorten challenge this common practice in his article.

With another edition comes the reality of the depletion of our article bank. As our current chapter president mentions, IT Governance is one of the important issues facing our profession. Articles in this area, especially those relating to UK and European experiences, would be most welcome. Please remember that if your article is published, you are able to claim CISA continuous education points for your efforts.

The Editorial Team is beginning to look at innovative ways to deliver Datawatch to our readers. Benefits would include more timely articles and more in-depth discussion of the issues presented in Datawatch – in all more value for your membership fee. This is not to say we will get rid of the trusted hardcopy: somehow tapping the scroll bar on your PDA does not quite compare to flipping the page, and one's partner may certainly object to the laptop been taken to bed as bedside reading!

Current email lists are an important component to enable us to utilise other electronic channels. About half our members are not receiving email notices from the chapter office because we either have no email address or we do not have their current email address. So, if you think this refers to you, please send the office your current details.

Finally, please feel free to use the old and trusted "Letter to the Editor" if you have any comments. The Editorial Team would love to hear from you.

On behalf of the team, Paul

London Chapter Events 2002/2003

Information Systems Audit and Control Association

26 September 2002	24 October 2002	28 November 2002	19 December 2002	23 January 2003
INTERMEDIATE - AUDIT	INTERMEDIATE - AUDIT/SECURITY	ADVANCED - AUDIT/SECURITY	INTERMEDIATE - AUDIT/SECURITY	INTERMEDIATE - AUDIT/FORENSICS
Information Governance (FSA, N2 & The IT Auditor) Vernon Poole KPMG 20 Farringdon St	Implementing IT Governance Paul Williams KPMG Salisbury Sq	Risk Management in 2003 Gareth Rowland ABN-Amro 250 Bishopsgate	Internet Threats & IDS Kenneth de Speigeleier ABN-Amro 250 Bishopsgate	Spreadsheet Fraud Ray Butler Venue to be confirmed
27 February 2003	**27 March 2003**	**24 April 2003**	**22 May 2003**	**26 June 2003**
ALL LEVELS - AUDIT/SECURITY	INTERMEDIATE - AUDIT/SECURITY	ADVANCED - AUDIT/SECURITY	ADVANCED - AUDIT/SECURITY	INTERMEDIATE - AUDIT/SECURITY
Information Security Speaker to be confirmed ABN-Amro 250 Bishopsgate	Control Over Internal & External Outsourcing Charles Mansour ABN-Amro 250 Bishopsgate	CRSA & the IT Auditor John Mitchell ABN-Amro 250 Bishopsgate	Data Protection - What's Coming Up & Implications For Systems (& AGM) Stewart Dresner ABN-Amro 250 Bishopsgate	E-Risk Revisited Speaker to be confirmed ABN-Amro 250 Bishopsgate

By the time you read this, the Xmas festivities will have been long gone, but hopefully you're ready to face the opportunities and challenges that 2003 will bring.

Website Goodies

As we head into 2003, it's a good idea to look at a couple of the lesser known ways that the benefits arising out of your membership of ISACA can directly assist you in your day to day tasks. For example:

- K-Net, your Global Knowledge repository www.isaca.org/knet, includes a growing number of downloadable Audit programmes at www.isaca.org/@member/auditprograms.htm
- Listserv, a discussion forum for any audit issues that you feel you need an airing with your fellow members at www.isaca.org/listserv.

If you haven't done so before, I think you'll find a visit to these sites both informative and rewarding.

IT Governance

Two topics that's fast becoming 'hot' (especially following the events at Enron et al last year are those of Corporate Governance in general and IT Governance in particular.

It's surprising how many directors of firms that know their up to the minute sales figures with an amazing degree of accuracy are unable to quantify how much their IT effort costs them over a year. Merely to ask a director the question 'about how much are we spending in IT on re-work every year?' (a cost that can often run into millions) is guaranteed to produce a high incidence of eyebrow raising, followed by a response along the lines of 'IT look after that sort of thing'. The foregoing is indicative of a lack of IT Governance

As you are probably aware, ISACA founded the IT Governance Institute (ITGI - web address www.itgovernance.org), its objective being the promotion of IT Governance, based on CObIT. .

IT Governance is basically all about the main stakeholders (executive and non executive directors)

- becoming involved in the way their firm's IT operation is conducted
- ensuring that the firm's IT effort is aligned with its overall strategy
- putting key measures in place to enable the key stakeholders in a firm to formulate what the firm expects from IT
- periodically asking the question 'how well are we doing?'
- putting corrective action in place where required
- measuring the extent of 'excellence' or otherwise by the use of 'maturity modelling'

In this way, it is possible to save significantly on the cost of IT and at the same time improve the service IT offers to the firm.

Obviously, to achieve recognition of IT Governance at the levels we seek, it will be necessary to raise awareness at senior levels within firms. To do this, we will need to market the concept of IT Governance in the coming year, both as a Chapter and as individual members. We have Gary Hardy, an experienced IT Governance practitioner, on board as our Chapter IT Governance 'Champion' and we are in the process of formation a Special Interest Group, which will focus on IT Governance and CObIT. Also planned for 2003 are initiatives aimed at key decision makers to 'sell' the concept of IT Governance.

It's easy to think that the whole concept of IT Governance is at too elevated a level for mere IT Auditors to become involved with. I disagree with that stance, because it is the specialist staff on the ground such as ourselves who are in an excellent position to influence and change minds. A good place to start is to look at the downloadable Briefing documents on the ITGI website.

If through 2003 we can see IT Governance, underpinned by CObIT implemented in organisations, we will have performed a significant service to the firm itself and also to the wider control community.

2003 Global Events

EuroCACS
23-26 March 2003
Grand Hotel Krasnapolsky
Amsterdam, Netherlands
www.isaca.org/eurocacs2003.htm
Member: US $1,345
Nonmember: US $1,545
Hotel rate: €175

NACACS
18-22 May 2003
Adam's Mark Hotel
Houston, Texas USA
www.isaca.org/nacacs2003.htm
Member: US $1,345
Nonmember: US $1,545
Hotel rate: US $139

International
20-23 July 2003
Grand Hyatt Singapore
Singapore
www.isaca.org/international2003.htm
Member: US $1,045
Nonmember: US $1,145
Hotel rate: Singapore dollars $250

Network Security
September 2003
Las Vegas, NV USA
www.isaca.org/nsc2003.htm
Member: US $1,095
Nonmember: US $1,195

Oceania CACS
22-24 September 2003
ANA Harbour Hotel
Sydney, NSW Australia
www.isaca.org.au

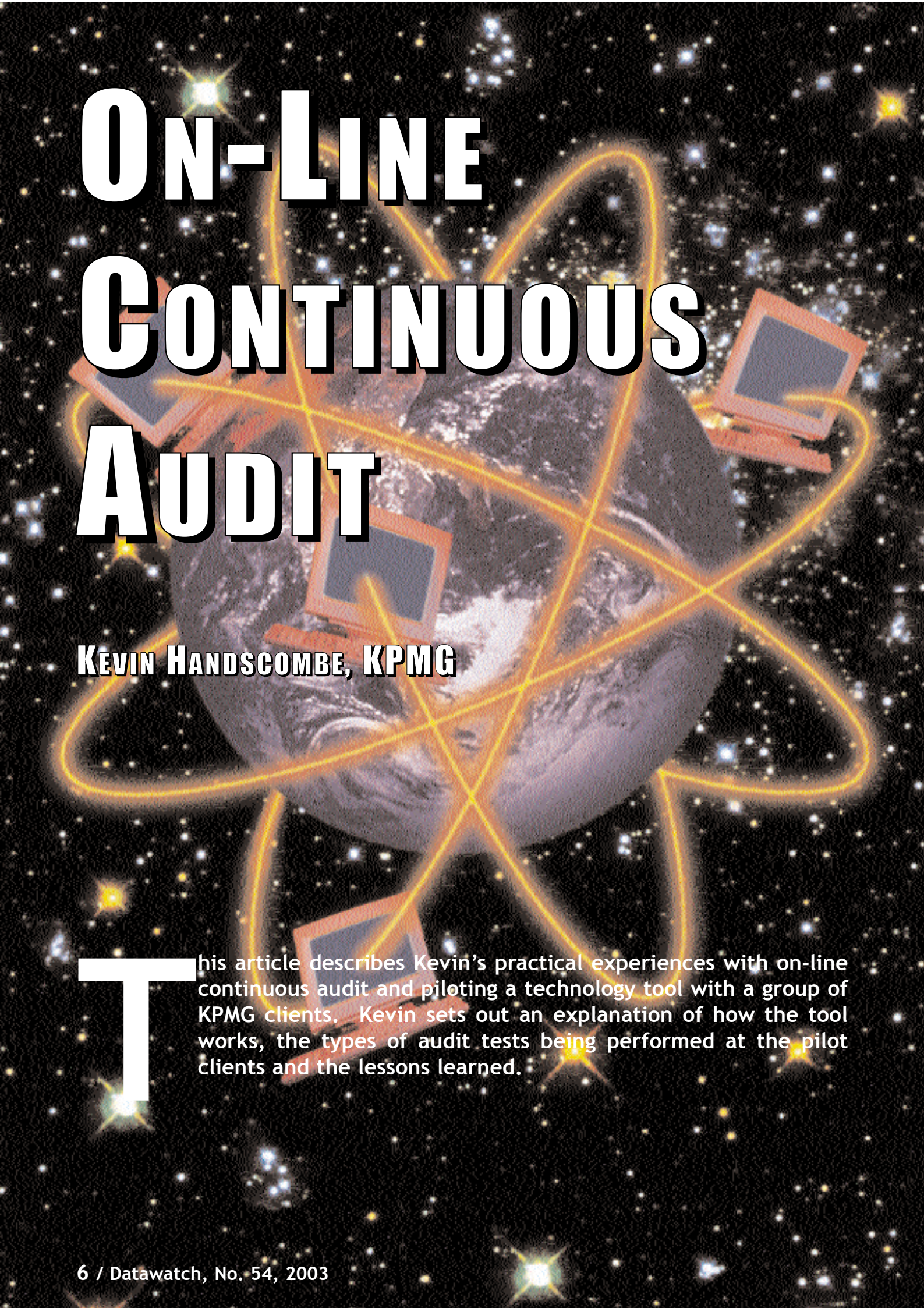
LatinCACS
October 2003
Sao Paulo, Brazil
Member: US $645
Nonmember: US $815
www.isaca.org/latin2003.htm

Network Security
November 2003
Milan, Italy
Member: US $1,095
Nonmember: US $1,195
www.isaca.org/nsc2003mi.htm

IS Audit & Control Week
January-June 2003
Melbourne, VCT Australia
Minneapolis, MN USA
Tampa, FL USA

IS Audit & Control Week
July-December 2003
Anaheim, CA USA
Ottawa, Ontario, Canada
Manchester, United Kingdom
Kansas City, MO USA
www.isaca.org/traiwk.htm

Information Systems Audit and Control Association®
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: conference@isaca.org
Web site: www.isaca.org



On-Line Continuous Audit

Kevin Handscombe, KPMG

This article describes Kevin's practical experiences with on-line continuous audit and piloting a technology tool with a group of KPMG clients. Kevin sets out an explanation of how the tool works, the types of audit tests being performed at the pilot clients and the lessons learned.

In selecting the tool to pilot, we wanted to solve the following issues:

- Extracting and transferring data to analyse is a complex issue, with the diversity of systems that our clients possess causing the expenditure of a great deal of effort to get data in a standard format. On top of this, there are hurdles to overcome such as encryption, firewall settings, data storage, Data Protection Act differences between countries, etc.
- We wanted to be able to audit controls as well as transactions to give a complete service. Analysing log files for evidence of the operation or failure of controls is not easy to automate and not all clients have their audit logs turned on all the time.
- Any solution had to have a minimal impact on clients due to their sensitivity to the risks and impact of pervasive connectivity, including negative effect on processing time, potential breach of privacy, loss of data, etc.
- Information Systems Auditors would be likely to be central to the delivery of any technology solution and it would be important for them to be integrated within audit teams. There has been an opposite trend to this for some time and we wanted to be able to reverse it.

We believe the key to the success of the pilot programme was the fundamental model we applied, which departed from conventional computer auditing models. There were three features to this model:

1 We do not extract volumes of client data for subsequent analysis. We connect directly to the data and monitor and analyse according to our requirements. Information which leaves the client premises is restricted in the first instance to test outcome reports. Two key advantages followed from this approach: we are able to deal with client concerns over loss of or damage to data, even where the client's data is so sensitive that they are not able to allow it to leave their site. Secondly, direct connection to the data allows us to monitor the operation of controls, through changes to database entries, flag settings or transactions. This is a strong proposition, and also overcomes the frequent obstacle to this kind of testing in that the relevant logs are switched off by the client.

2 By using JDBC and ODBC connectivity and standardised drivers, we are able to work with any reasonably modern system with a database behind it. In this way, we can access all the databases available, particularly where there are diverse (and possibly not integrated) systems. We can also simultaneously access financial and non-financial systems and make it easier to examine analytics or carry out environmental audits

3 Finally, by using a tool with an intuitive GUI interface, we had something that General Auditors could use, but which could also be used in more sophisticated ways by 'power user' Information Systems Auditors.

The model explained

The model we used in the pilots solved these issues and is summarised in the diagram on page 8.

Technical installation

1 The tool is pre-installed on a PC, which is the audit firm's property. It remains at the client premises in a secure location, such as the computer room.

2 In this way, we make use of the client's security procedures and firewall.

3 The PC is linked to the client's network with a connection like any other client user PC. In setting up and configuring the PC, all that is required is:

- A network user ID and password
- An email user account
- A database user ID and password (to give read only access)
- IP address of the database(s) and email servers

The tool handles all the connectivity and provides an on-screen database schema, listing all the tables in the database and the fields within the tables. An intuitive GUI interface provides point and click selection of tables, fields, filters, operands and table joins. In this way audit tests can be built, or templated tests can be edited to set parameters as desired.

4 The PC monitors the client's databases for specified changes or interrogates them on a scheduled basis. When a database change occurs which creates an exception event, the tool notifies the audit team with the results by email. (See Fig 2 on page 9.)

5 Different members of the team can receive personalised emails, depending on their area of interest or the materiality they might apply to exceptions.

6 We typically also copied the email to local management and/or Internal Audit. In our pilot programme we integrated client management within the process so that the exception would have already been investigated and resolved before we contacted them with our enquiry.

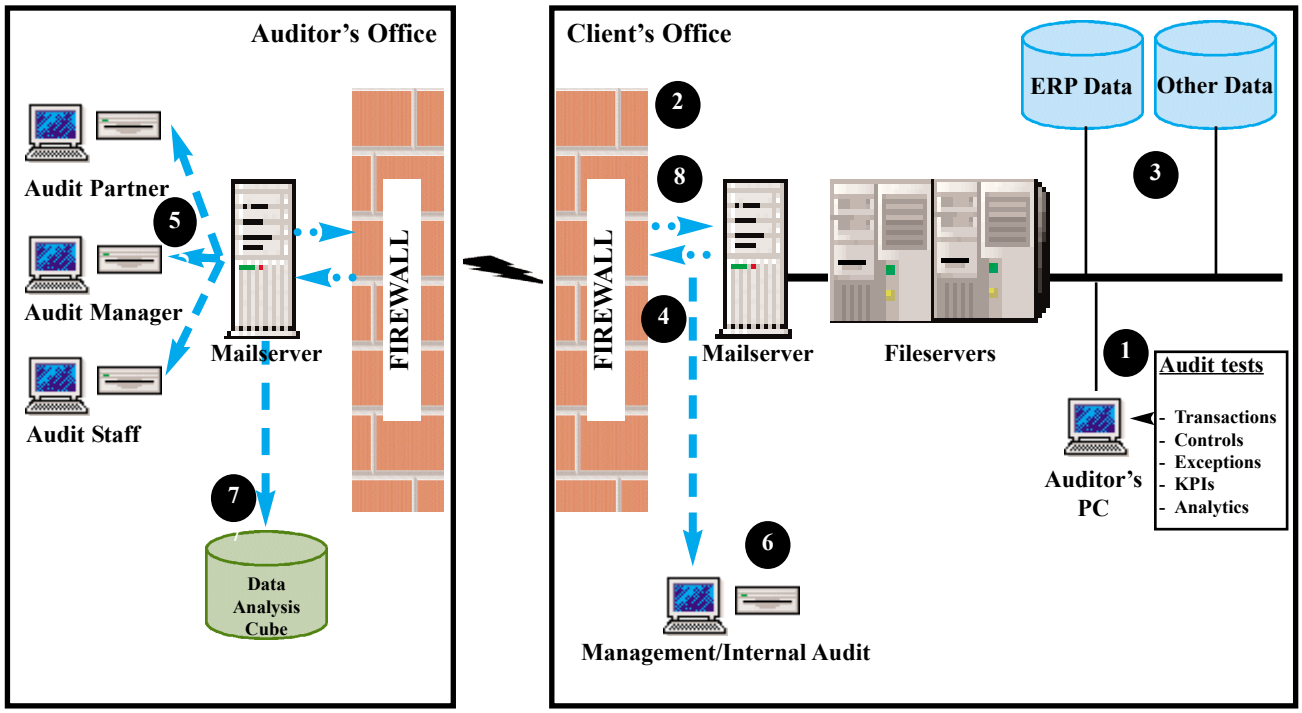


Fig 1: Overview of the KOLA model

7 'In addition to testing outcome reporting, it is also possible to extract information, such as Key Performance Indicators (KPIs), on a regular basis using a scheduler, and send it to the audit team as a simple email attachment. This could be entered into a database for further analysis and for benchmarking.

8 The tool can also 'listen' for incoming emails from the audit teams containing parameters to include in on-demand exception reports or data extract queries.

Comparison with other tools

The tool is similar in concept to others available with ERP systems, such as Oracle Alerts. The main difference is that it is a generic tool that can work with any database and is not package-specific. This enables access to all the databases that the client uses, including non-financial systems.

Another difference is that it does not rely on database triggers, although it can use them. Triggers are a useful method for monitoring database changes, but are not easily implemented because many clients' IT policies do not permit them.

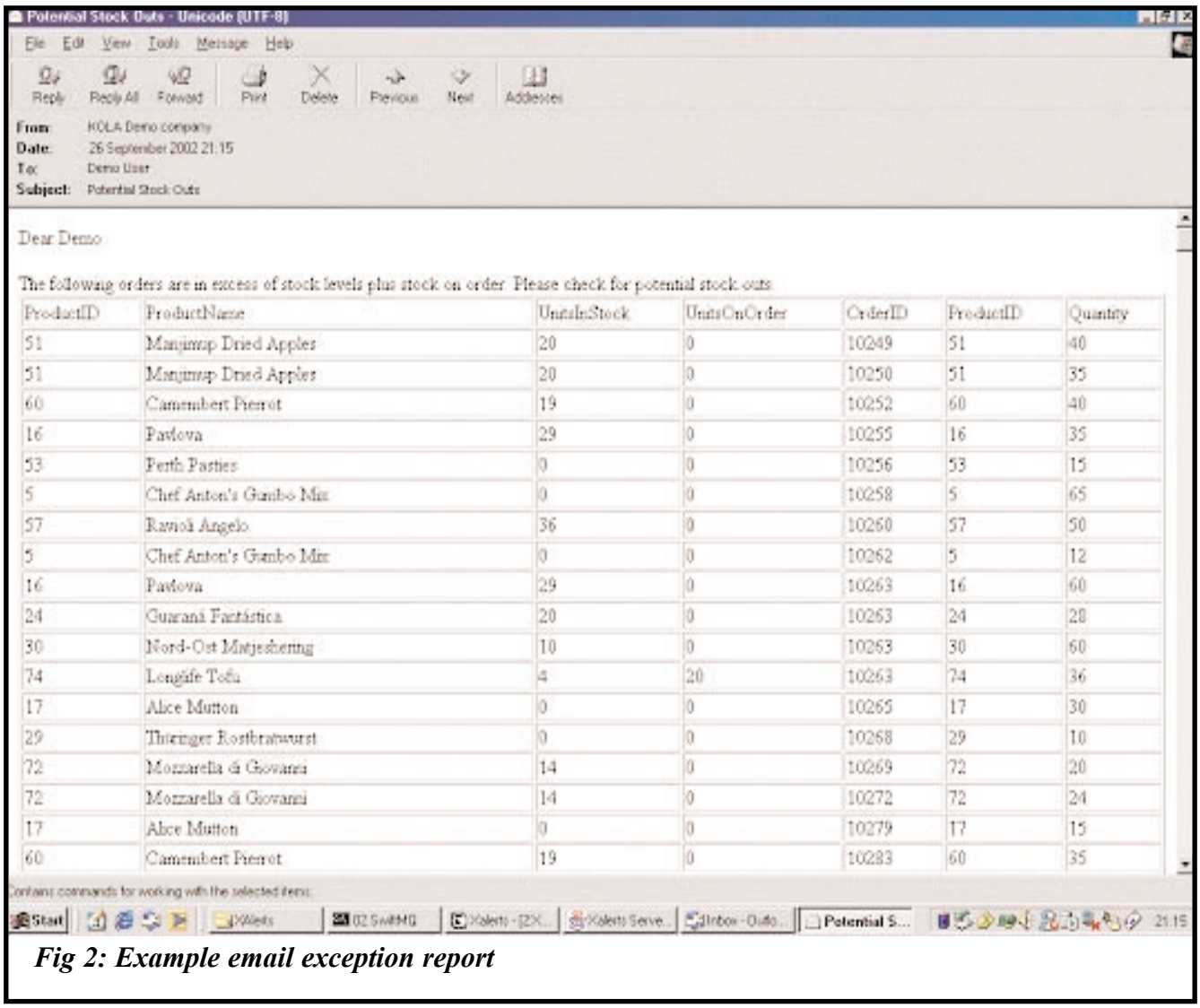
Client reaction case studies

We piloted the tool with a number of clients, both financial statement audit and outsourced internal audit, covering a range of sizes and industry types. As mentioned in the Introduction, one of the key issues we had to deal with was mitigating client concerns about potential threats to data integrity. Of course, in the practical situation of persuading a client to take part in a pilot programme, there are additional hurdles to deal with. In fact we found that the model we used presented was well received for a number of reasons:

- We would not load any software on their system
- We would not be a drain on their IT department as the tool can analyse the database schema and allow us to be largely self-sufficient in selecting tables and fields to audit.
- The client would be involved in the alerting process and informed about problems as they happened. The introduction of a time delay between initial reporting and follow-up by the auditor gave the clients time to address any issues. They responded very positively to the idea of proactive intervention rather than the conventional approach of pointing out errors long after the event when it is too late for corrective action.

In selecting the pilots we were interested in trying out examples of the following types of audit test:

- Regular extraction of KPI data to give information on how the client's business is progressing.
- Ad-hoc remote extraction of data using the email listener to investigate exceptions.
- Testing controls through monitoring changes to standing data masterfiles, such as authorization limits and price lists.
- Monitoring unusual transactions, such as adjusting journal entries above materiality or



Potential Stock Outs - Unicode (UTF-8)

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: KOLA Demo company
Date: 26 September 2002 21:15
To: Demo User
Subject: Potential Stock Outs

Dear Demo

The following orders are in excess of stock levels plus stock on order. Please check for potential stock outs:

ProductID	ProductName	UnitsInStock	UnitsOnOrder	OrderID	ProductID	Quantity
51	Manjimup Dried Apples	20	0	10249	51	40
51	Manjimup Dried Apples	20	0	10250	51	35
60	Camembert Pierrot	19	0	10252	60	40
16	Pavlova	29	0	10255	16	35
53	Perth Pasties	0	0	10256	53	15
5	Chef Anton's Gumbo Mix	0	0	10258	5	65
57	Ravioli Angelo	36	0	10260	57	50
5	Chef Anton's Gumbo Mix	0	0	10262	5	12
16	Pavlova	29	0	10263	16	60
24	Guaraná Fantástica	20	0	10263	24	28
30	Nord-Ost Matjeshering	10	0	10263	30	60
74	Longlife Tofu	4	20	10263	74	36
17	Alice Mutton	0	0	10265	17	30
29	Thüringer Rostbratwurst	0	0	10268	29	10
72	Mozzarella di Giovanni	14	0	10269	72	20
72	Mozzarella di Giovanni	14	0	10272	72	24
17	Alice Mutton	0	0	10279	17	15
60	Camembert Pierrot	19	0	10283	60	35

Contains commands for working with the selected items.

Start | XAlerts | 02 SwitMG | XAlerts - [ZX... | XAlerts Serve... | Inbox - Outlo... | Potential S... | 21:15

Fig 2: Example email exception report

involving posting to unusual accounts.

The following examples illustrate the methodology developed:

Case Study One

A large diversified world wide group with management accounts data held at headquarters. The assignment is a financial statements audit. The pilot tests include:

- Monthly extract of KPI info for group companies into a spreadsheet sent as an email attachment, compared to budget, with major variations highlighted with 'traffic light' colour coding. This has saved the audit manager time in reviewing results, has highlighted problem issues early for raising with management and has helped modify audit scope for overseas teams. The traffic light report helped the audit manager spot issues much more quickly than with conventional management accounts - in half an hour rather than two to three days. The client also liked the simplicity and flexibility of the spreadsheet and asked for it to be sent to them as well each month.
- On-demand extract of KPI data, triggering a query by sending an email containing company number, period and account number parameters. This enabled additional management accounts data, in addition to the pre-defined KPIs, to be extracted when needed.
- Monitoring of the company details masterfile for any new acquisitions. This is an example test of standing data checking and helps the audit manager identify new audit requirements that he hasn't been notified about. He was able to contact the local office in good time and begin planning an audit team, stock take attendance etc. This has proven useful in picking up where the client has bought new subsidiaries, but forgotten to inform the audit manager.

Case Study Two

Implemented at one subsidiary of a large group where we have an internal audit outsourcing

contract. The project is supported by the group Head of Internal Audit, who is able to monitor the group. The pilot tests include:

- Monitoring accounts payable standing data, checking for changes to names, addresses, bank details etc as possible indicators of fraud.
- Monitoring changes to sales price masterlists for unexpected amendments.
- Checking sales order entry transactions for input errors (eg non-numeric data in numeric fields, spurious data, suspiciously low values). This is not an audit test, but was included at the suggestion of management to test the capability of the tool, and to fill a controls gap. The objective was to identify regular offenders who need either additional training or reminding of company policies. This should improve order entry efficiency, reduce the invoice rejection rate of customers and give an improvement in cash flow.

Case Study Three

A high tec manufacturing company. Another financial statements audit, this time dealing with a 'modern' (warehouse) database system and an older (accounting) system using indexed sequential files. This tested the tool's capability in dealing with legacy flat file systems. The pilot tests included:

- Checking the correct operation of the interface between the warehouse system and the accounting system by comparing the inventory quantities in each and reporting differences
- Monitoring the inventory standing data and reporting unexpected changes to standard costs.

Impact on Information Systems Audit

The installation process is quite short, probably no more than half a day, but involves a degree of liaison with the IT department, which is a job done best by Information Systems Audit. It is necessary to identify the type of system the client is running and to install the necessary drivers to ensure connectivity.

Knowledge of data structures and query languages can be helpful in designing tests and making sure they run in the right way. These are skills that are being acquired increasingly by General Auditors, but there is a training and advisory role that IS Auditors can still fulfil.

The most difficult part of running the pilots that we found is identifying the data tables needed. Most ERP packages come with a standard set of tables, many of which are not used and make it more difficult to spot the ones the auditor is interested in - you 'can't see the wood for the trees'. Experience in dealing with the set up and configuration of ERP systems reduces the reliance on the client's IT department for help. This can be important where IT systems have been outsourced, because any help from the outsourcer tends to come at a price.

In a similar vein, the sheer multiplicity of data tables can make it difficult for the team to set test objectives and define routines. Laying all the company's databases open to interrogation, including non-financial systems which may not have been accessed before, can create so much choice that it's hard to know where to start. It may be better to have a templated list of standard tests: this is not necessarily a retrograde step, due to the ease with which tests can be customised and new ones built. The art is in good design for the standard test list for the audit team to choose from. This is an issue to work out in subsequent piloting.

And finally .....

A major benefit that I foresee, particularly for the CISA community, could be that computer auditing becomes 'sexy' again, it could come back in fashion and really be a key part of the audit.

It has often been a problem to integrate computer auditors into the audit team. The term 'Computer Auditor' tends to have a number of connotations. Under cost pressure, audit managers don't often see the value of giving up budget to fund IT activities. And it has often taken substantial amounts of time for the IT auditor to get the data downloaded from the client in the right sort of format and on the right sort of tape cartridge. Then behavioural issues come into play which often affect a smaller, technically focused sub-group within a team, dealing with processes which other team members don't understand and, being intangible, can't touch and trust.

An on-line audit tool could help overcome these difficulties, because it gives the IS Auditor and the non-IT specialist Auditor a common tool and a common language. The non-specialist can use the tool in 'point and click' mode to build straightforward tests from on-screen choices. The IS Auditor can do more 'industrial strength' work by writing queries directly, rather than menu short cuts. But they are both working with the same tool. The Computer Auditor retains a bit of mystery about what he or she does, but not that as much as before because the non-specialist has enough knowledge to start asking questions about what he's getting for his money.

Kevin Handscombe is a Senior Manager with KPMG and is a member of Assurance Support & Innovation.

Kevin.Handscombe@kpmg.co.uk

Mother's Maiden Name?

I was registering a new credit card the other day, and the subject of security was raised.
The operator asked how would I like to identify myself when I ring in to transfer funds to and from the card.
As a good security professional, I had ready a long word, a place, and a date.
The operator just requested my Mother's Maiden Name!

Brian Shorten

Asking around, it seems that this is still the most popular way to authenticate a telephone caller.

Am I the only one who can see the flaws in this old favourite?

A password must be confidential, Mother's Maiden Name is not a secret; anyone can find a person's mother maiden name, given enough incentive. In fact, your mother's maiden name is on your birth certificate!

Some Latin countries use the Mothers maiden name as part of the child's full name. Spain uses paternal last name followed by maternal last name separated by a hyphen or the letter 'y'. Portugal uses maternal last name followed by paternal last name. So in both cases it is easy to find out the mother's maiden name from documents and databases.

Many people now compile and publish their family tree on the Internet, showing first and last name for each preceding generation, including the maiden name of all female ancestors.

Most employers keep a next of kin list, just in case they need to make contact in an emergency.
For many people, next of kin is mother, and the name is available to everyone with access to the list - an unknown number, possibly everyone in HR. Obviously, members of the family know the name - what about ex-partners, who may be tempted to use the card, or make changes to the account, for a variety of reasons, including good old revenge?

A 'password' should not be easy to guess.
Although some people have an unusual last name, many have a common one. In many cases, it would be possible to guess at SMITH, JONES or PATEL, and be successful.

Passwords must expire on a regular basis and be renewed. This is to prevent unauthorised access by guesswork.
The most common standard is for a password to expire every 30 days; by definition, a mother's maiden name cannot expire.

And another thing .... As the number of marriages drop, and the number of women who change their last name on marriage diminishes, the concept of 'maiden name' disappears as many people have the same last name as their mother.

So what is the answer?

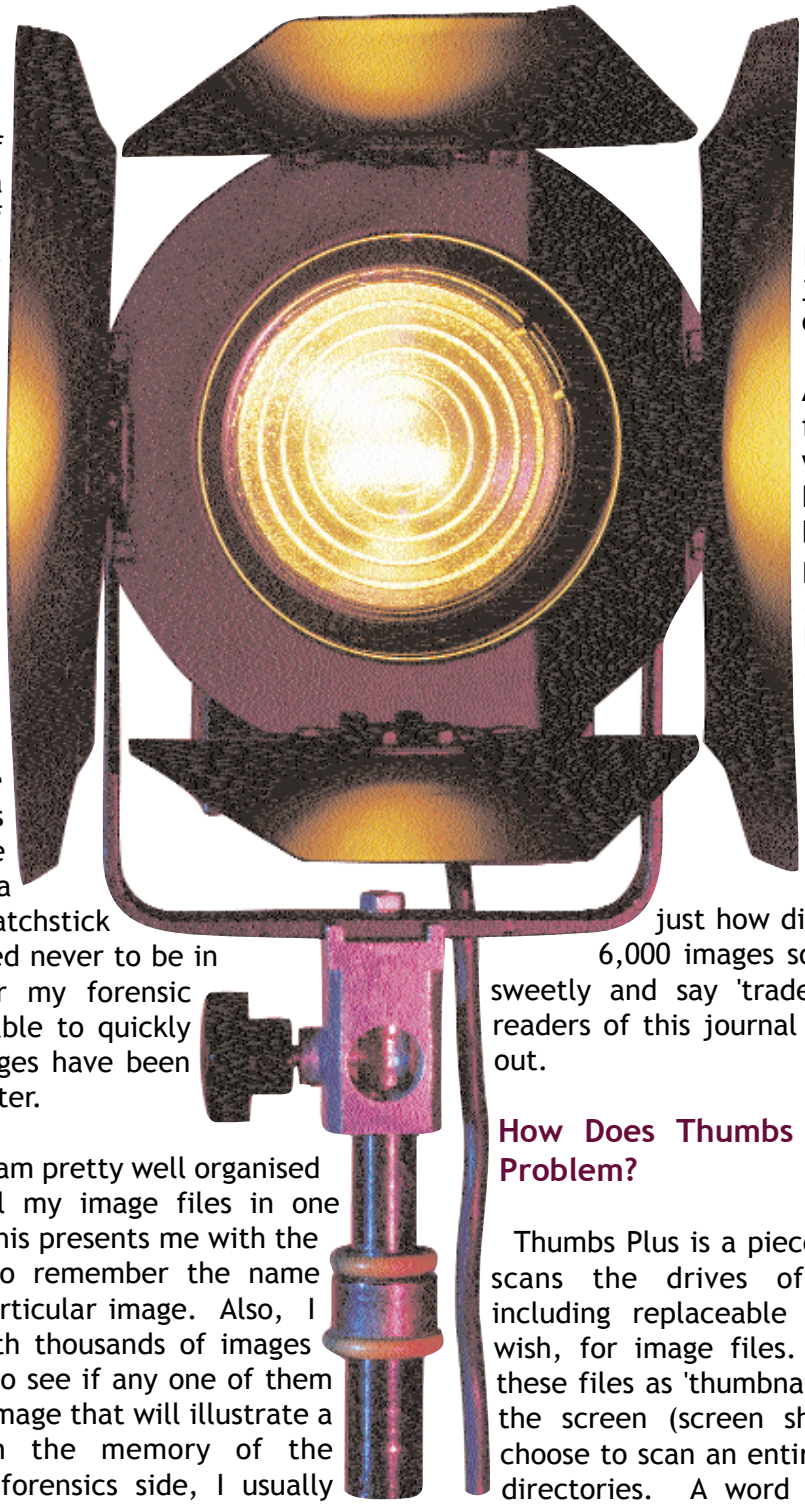
I believe we should refuse to accept the use of Mother Maiden Name as a password. Whenever we audit an application, which uses Mother Maiden Name as part of an authentication process, we should raise an audit point and make a strong recommendation that a more realistic process be used.

What do others think?

Am I being paranoid, or is there a valid security point that I am missing?

SOFTWARE SPOTLIGHT "THUMBS PLUS"

JOHN MITCHELL



The Problem

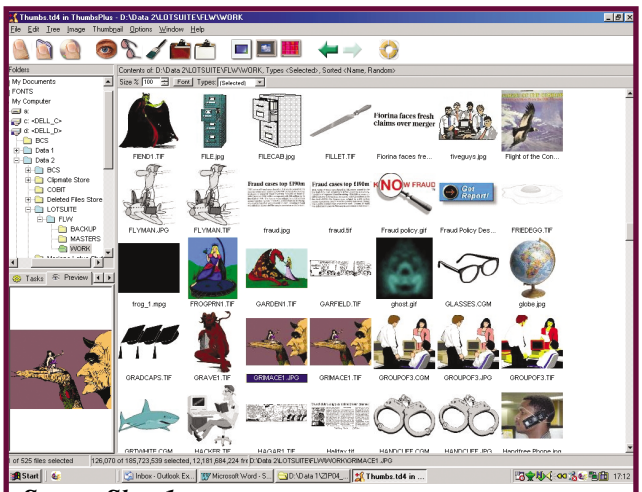
I do a lot of presentations and a fair amount of computer forensic work. What do these two have in common? Well, they both require me to know what image files are available on a particular machine. For presentations, I like to add more than the standard clip art to my visuals (I once attended a presentation when the person next to be groaned out loud as yet another slide appeared with a Microsoft Office matchstick man on it and I vowed never to be in that position). For my forensic work I need to be able to quickly determine what images have been stored on the computer.

Take my situation. I am pretty well organised and try to store all my image files in one directory, but even this presents me with the problem of trying to remember the name associated with a particular image. Also, I have lots of CDs with thousands of images that I need to scan to see if any one of them has that 'knock out' image that will illustrate a point and stick in the memory of the audience. On the forensics side, I usually need to evaluate the entire machine and its removable media knowing that the machine's owner is unlikely to have named a file 'child pornography 876' just to help me out.

A few years ago I found Thumbs Plus which I now use to help me solve both of these problems. Indeed, I often have people coming up to me after a presentation asking where did I get the fabulous clip art from, or lawyers enquiring just how did I evaluate those 6,000 images so quickly? I smile sweetly and say 'trade secret', but for readers of this journal the secret is now out.

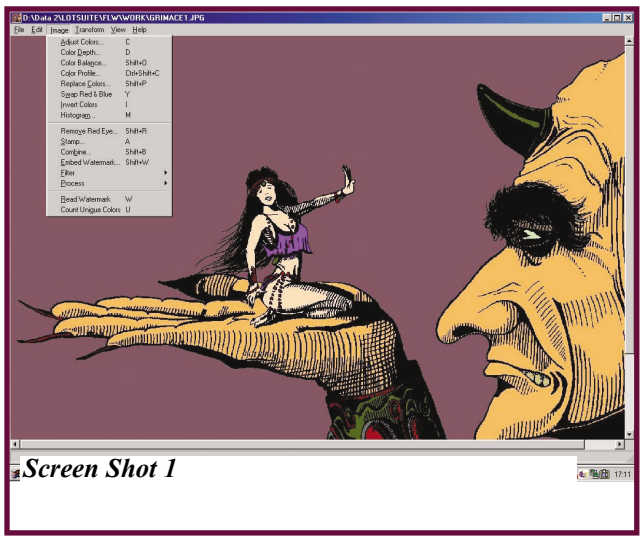
How Does Thumbs Plus Solve the Problem?

Thumbs Plus is a piece of software that scans the drives of your machine, including replaceable media if you so wish, for image files. It then displays these files as 'thumbnail' size pictures on the screen (screen shot 1). You can choose to scan an entire disk, or specific directories. A word of warning here. Creating thumbnails for an entire disk takes a



Screen Shot 1

considerable amount of time and appears to be memory intensive. You can also scan network drives, so you can view and copy images from any machine on the network. providing you have the necessary permissions.



Screen Shot 1

Once the thumbnails are created you can select them for further editing (screen shot 2). Thumbs Plus comes with quite powerful image manipulation tools and you can save the edited image as a different file type to the one that you opened. I find this particularly useful as I have standardised on compressed JPEG as my favoured image file type. The file types supported by Thumbs Plus are listed in the table.

If you add, or delete files, outside of Thumbs Plus, then you will need to do a rescan when you next load the software, but you can also set an option to 'watch' selected directories and have Thumbs Plus do the process automatically. Personally, I now do all my image manipulation, including deleting files, from within Thumbs Plus as it prevents me from inadvertently deleting an image that took me ages to find in the first place.

The software also enables you to scan images into the machine and to create a slide show from images in a particular 'gallery'. A gallery is a logical collection of images. This means that if you have inadvertently left your copy of Freelance, or PowerPoint at home you can quickly create a slide show based around the images stored on your computer. Its selection of slide transition options is so good that onlookers will be unaware that you are not running normal presentation software.

Batch processes allow you to operate against all, or selected images, in one pass without the need to view each image separately. So if you want to convert all those TIFs to JPEGs, just set up the relevant batch command and let Thumbs Plus get on with it.

This is a truly impressive piece of software that should be part of every computer auditor's tool kit.

Functionality	*****
East of Use	*****
Support	*****
Value for Money	*****

Platforms: Windows 95/98/Me/NT4/2000/XP

Vendor: Cerious (www.cerious.com)

Version: 5.01

Price: £49.00 plus VAT

John has no financial or other interests in the software reviewed by him. His views are his own and do not necessarily reflect those of the London Chapter of ISACA. John takes no responsibility for any harm suffered to an individual, organisation, or system as a result of his views.

NETWATCH

ALLAN BOARDMAN takes a look at some of the online resources available to audit, risk and security professionals to enable them to keep in touch with the main news stories relevant to their jobs. This is just a taster and no doubt many readers will have their own favourites. Please feel free to advise Allan of any online newsletters that you feel may be of relevance to other Datawatch readers.

SANS Institute offers three different free weekly electronic subscriptions:

- SANS NewsBites - key computer security stories.
- Critical Vulnerability Analysis Newsletter - focuses on the main vulnerabilities, tells what damage they do and provides data on the actions organisations have taken to protect themselves.
- Security Alert Consensus - a weekly summary of new alerts and countermeasures each week with announcements from: SANS, CERT, GIAC, NIPC, DoD, Security Portal, Ntbugtraq, Sun, Microsoft and several other vendors. Can tailor and customise to select only operating systems you want included in your customise weekly digest.

Further details here:
http://www.sans.org/sansnews/

Common Vulnerabilities and Exposure (CVE) offers announcements and updates via its e-newsletters.

- CVE-Announce is for those interested in general news about CVE, such as new versions, upcoming conferences, new Web site features, etc. Messages are sent infrequently, once a week or less.
- CVE-Data-Update provides subscribers with reports of new CVE entries and/or candidates, and other detailed technical information regarding CVE. This list is intended for heavy technical users of CVE, such as vulnerabilitydatabase maintainers, or those who require timely notification of new candidates.

For further details, visit:
http://www.cve.mitre.org/signup/register.html

SecurityFocus offers the following weekly newsletters SecurityFocus News, Microsoft Security News, Linux Security News.

Details at:
http://online.securityfocus.com/archive

SecurityFocus also hosts a number of mailing lists dedicated to specific security topics, including the following focus areas bugtraq, ids, linux, ms, sun, unix-other, virus, forensics, honeypots, incidents, secnews, pen-test, secevents, sectools, vpn ,Web Application Security, auditing, certification, cryptography, firewalls hacking, intrusion detection, law, operating systems, privacy, products, projects, vulnerabilities, web, Visit:
http://online.securityfocus.com/cgi-bin/sfonline/subscribe.pl
for more details.

ITsecurity.com produces a regular digest, Security Clinic Digest and a weekly newsletter,

The News. Details at:
http://www.itsecurity.com/tecsnews/news.htm

The CERT Advisory Mailing List is used to notify subscribers of computer-related security problems and issues. Both advisories and summaries are sent out. To subscribe to the CERT advisory mailing list, send email to majordomo@cert.org, and in the body of the message, type subscribe cert-advisory or visit http://www.cert.org for details.

Security Wire Digest is an e-mail newsletter brought to you on Mondays and Thursdays by Information Security magazine. For details, visit:
http://www.infosecuritymag.com

SC Infosecurity Opinionwire and Newswire newsletter comes to you from SC Magazine. For details, visit:
http://www.westcoast.com/subscribe_infosecnews.html.

Microsoft Security Notification Service provides summary information from every Microsoft security bulletin. Security bulletins are technical documents discussing newly discovered security vulnerabilities,
and provide information on what products are affected, the risk the vulnerabilities pose, and how to eliminate them. To subscribe to the Microsoft Security Notification Service, visit:
http://register.microsoft.com/regsys/pic.asp

Linux Security has a number of discussion and mailing lists, including:

- Linux Security Discussion List for general security-related questions and comments
- Weekly Security Advisory Watch This mailing list is a comprehensive overview of the security vulnerabilities that have been announced for the week. It includes pointers to updated packages and description of the vulnerability.
- Weekly Security Newsletter. This weekly newsletter captures all the most relevant and important security events that affect the Linux and open source community.

Visit:
http://www.linuxsecurity.com/general/mailinglists.html for further details.

AccountingWEB publishes a range of regular newswires, including IT Zone Newswire. Details here:
http://www.accountingweb.co.uk/

The Institute of Internal Auditors produces a weekly IT Audit newsletter. For a free subscription visit:
http://www.theiia.org/itaudit/.

Risk Audit has a daily news service called Stop Press aimed at individuals involved in corporate governance. Visit www.riskaudit.co.uk for more details.

This site gives an extensive list of online security bulletins, mailing lists, newsletters and discussion groups:
http://lists.insecure.org/.

Note: This page is also available online as an html page at:
http://www.isaca-london.org/netwatch.htm
to enable readers to easily use the web links.

EUSPRIG III - SPREADSHEET RISKS - THE HIDDEN CORPORATE GAMBLE

Ray Butler

The 3rd European Spreadsheet Risks Information Group conference was held in July in Cardiff. ISACA Northern England chapter was the main sponsors of the event, which was also supported by Lloyds TSB, KPMG and the British Computer Society.

It attracted academics and practitioners from Australia Austria Canada Ireland, the UK, and the UK. Visit www.eusprig.org for the programme and abstracts of the papers.

It's hard to pick out particular gems from such a good programme, but highlights for me were:

- The challenging *Spreadsheet Engineering: A Research Framework* from Tom Grossman, University of Calgary and founder of the North American equivalent of EuSpRIG.
- A fascinating history of the Spreadsheet (Which an be brutally summarised as VisiCalc to Excel via 20 bankruptcies) from Martin Campbell-Kelly of Warwick University.
- The announcement of an Asia - Pacific equivalent of EuSpRIG
- The conclusion from the closing panel discussion that we should set the research and publicity agenda firmly on improving productivity from and quality of spreadsheets in business rather than beating the drum about errors.

More questions than answers arose from the conference.

We know that spreadsheets are dangerous, we know it's difficult to get managers to take them seriously, so the key message is that we need more research on the impact and incidence of spreadsheets in organisations - Who uses them, What they are used for, the exposure of companies to error, what training users have / what training do they need, how formal should controls be - And should they be applied to ALL spreadsheets in an organisation, and if not, which ones ?

If your organisation can contribute information or money to finding out, EuSpRIG is keenly waiting to hear from you. Find out more from the Web Site.

CISA Training 2003

Information Systems Audit and Control Association

The London Chapter is pleased to announce that in 2003, not only will we offer our well established CISA review weekend workshop, but we will also provide formal training for each of the CISA domains. This additional opportunity to enhance your knowledge in order to help you pass the examination will be provided as 4 one day events. You can either attend all of the days (and receive a 10% discount on the individual day cost), or book individual sessions to suit your particular training needs. All training will include a printed delegate pack and all refreshments.

A maximum of 24 delegates can be accommodated for each training day and the weekend workshop and there is certain to be a huge demand, so book early to guarantee your place.

Venues & Accommodation

Training day sessions will be held in the superb Quorum Training facilities at Tavistock Square, near Euston, in London.

The Residential workshop will be held at KPMG's superb training facilities at Wokefield Park, near Reading.

Email Nancy (nancy@isaca.org.uk) for further details and a registration form

21 January 2003

DOMAINS 1 AND 6

- The IS Audit Process (10%)
- Business Application System Development, Acquisition, Implementation & Maintenance (16%)

25 February 2003

DOMAINS 2 AND 3

- Management, Planning & Organisation of IS (11%)
- Technical Infrastructure & Operational Practice (13%)

31 March 2003

DOMAIN 4

- Protection of Information Assets (25%)

30 April 2003

DOMAINS 5 AND 7

- Disaster Recovery & Business Continuity (10%)
- Business Evaluation & Risk Management (15%)

10 - 11 May 2003

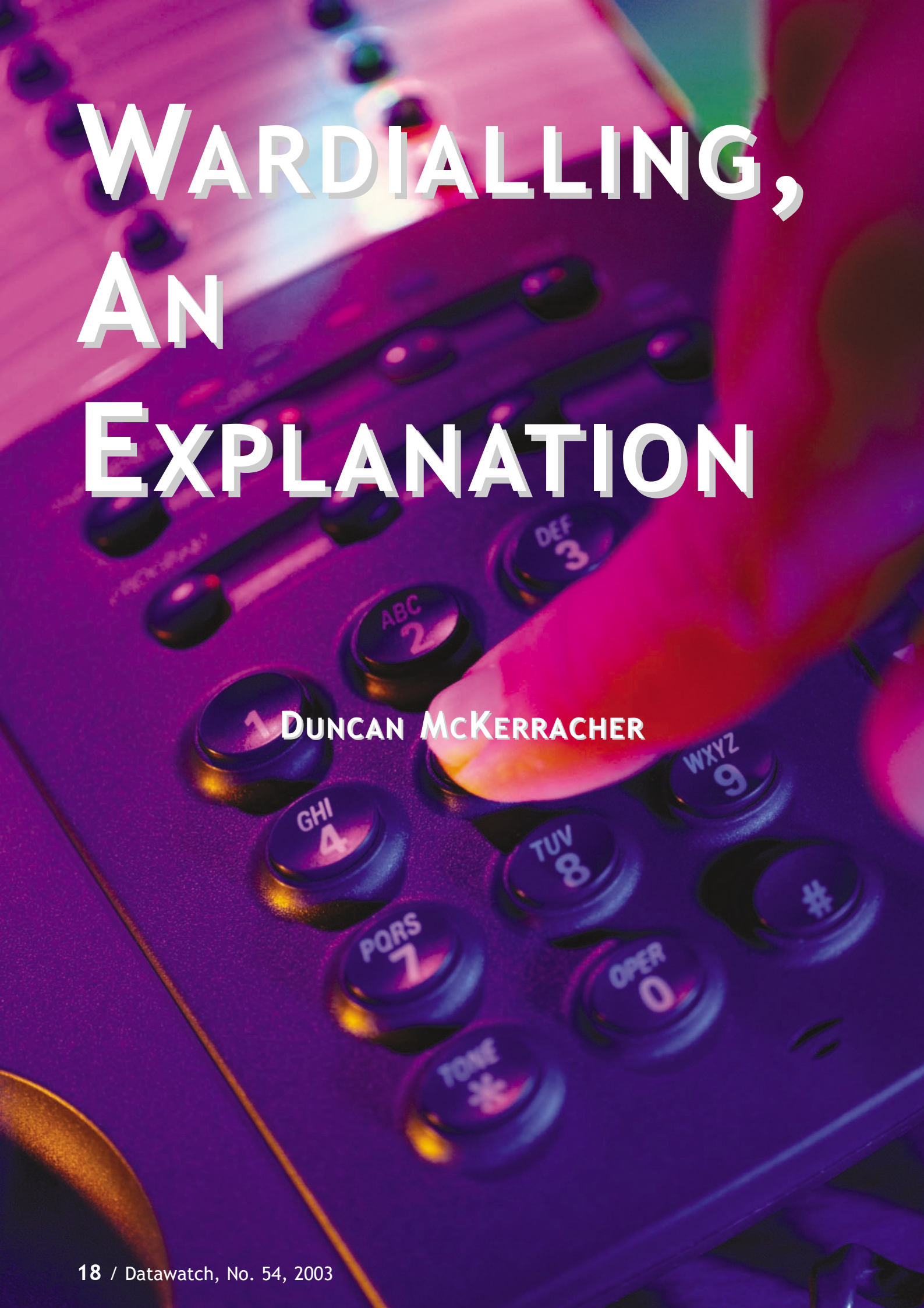
CISA REVIEW WEEKEND

The CISA Review Workshop is a separate chargeable event and its intention is to enable a delegate to identify any particular weaknesses in time to allow remedial action before the CISA examination. The format is primarily a reminder of the core subjects in each domain followed by a mock examination. The actual CISA examination is scheduled for Saturday 14 June, so delegates have a full month to review any weaknesses identifed during the workshop.

The workshop includes Saturday night accommodation and meals.

Wardialling, An Explanation

Duncan McKerracher



What is Wardialling?

Wardialling is the act of dialling a range of telephone numbers in order to identify services such as modems and secondary dial tone. Essentially, wardialler is a piece of software that can be configured to activate a modem to dial a sequence of numbers, and make a record of the response to each call.

Wardiallers have long been used by the hacking community to penetrate both voice and data networks. However, wardialling is also an important tool for network managers in an attempt to discover vulnerabilities of their network. It is fundamental in the fight against network hacking and is increasingly used as the first step in a penetration test.

Illegal Wardialling

There are two types of illegal users of wardiallers, these are usually grouped under the misleading heading 'hackers', however that term is ambiguous and does not necessarily refer to someone with malicious intent.

The more correct terms are 'cracker' and 'phreaker'. A cracker would use wardialler to identify modems prior to attempting to penetrate a data network. This lays the groundwork for an attempt to break into a data network and would detail all active modems connected to an organisation's PABX. A "brute force" attack would be the next avenue of investigation to a cracker involving the use of 1,000's of combinations of user-name and passwords stripped from a dictionary compiled specially for this purpose.

A phreaker uses wardialling to identify secondary dial tone in order to perpetrate toll fraud against a poorly configured PABX. Once secondary dial tone has been discovered, the phreaker will be able to make as many fraudulent calls as he wishes. Typically these calls will be made to premium or international destination thus incurring large costs to the victim.

Wardialling Software

A large variety of wardiallers are available on the Internet via numerous hacking web-sites, however caution should always be taken when using such sites as there is great potential for downloading 'malware'. This 'malware' will most usually take the form of viruses, although recently the greatest threat has been represented by 'trojans', malicious programs contained within more innocuous ones that will open 'back doors' to a once secure network.

Most wardiallers are written in MS-DOS and are several years old. These are not complicated tools and so have not required any upgrading or added functionality as the principles of wardialling have remained the same for many years.

The software randomly dials numbers from a specified range and records the response it receives, these can be:

- Dial Tone
- Modem
- Timeout (Unanswered Call)
- Busy (Line in Use)
- Fax

Wardialling your own network

It is important to carry out a wardialling exercise on your own network to identify unauthorised modems and secondary dial tone. It is obviously important to do this before a cracker or a phreaker does. In effect, this represents the initial step in carrying out a penetration test. Dial tone can detected if your PABX is poorly configured and modems can be detected if staff have introduced modems without prior approval.

Wardialling a range of DDI numbers should be carried out twice, first of all during the day and again at night. This approach is taken to identify if any modems, unauthorised or otherwise, are active only at night when employees are most likely to use remote access.

It is essential that all organisations carry out a wardial such as this at least every six months. This will ensure that a much tighter standard of security is maintained. As modems and inter-computer communications become more commonplace and therefore more familiar to end-users, potential vulnerabilities such as unauthorised modems increase.

Once you have carried out a wardial of your own network it is important to analyse the results and to carry out the following recommendations:

- Authorised modems must be re-assessed as to their security settings and validity (The most secure way to approach this problem is to remove as many modems as possible.)
- Dial-back modems should be introduced meaning that the modem is activated from an outside line as usual, but it will drop the connection as soon as it is made. The modem then dials back a pre-determined number.
- All unauthorised modems that have been identified must be removed immediately.
- Once modems have been removed, a global announcement should be made explaining the dangers of such equipment to the integrity of a data and voice network.
- A standalone PC connected to a DDI extension via a modem is avery effective way of detecting a malicious wardial. These PCs act as ‘honey pots’. Once one is detected, and attempt to break in is carried out, it can send an email to a particular address that will set off the network administrator’s pager.

Duncan McKerracher is an independent consultant specialising in voice and data network security.

Business Continuity Planning in an E-commerce Environment

Steven Ross, Sandra Allison and Simona DeFeo,
Deloitte & Touche and
James Barnes, CAN

Reviewed by John Mitchell

This book has 7 major sections. A general introduction that puts the book into context and which specifies the differences between Disaster Recovery Planning (DRP) and Business Continuity Planning (BCP). This is followed by Business Continuity Planning and E-Commerce which contains a couple of useful tables showing the average hourly financial losses incurred in different business sectors as a result of a system failure and exactly what an availability percentage really means (an availability of 99.9% means that your are down for nearly 9 hours a year, which may not be good news if it is Christmas Eve and you retail Christmas trees). This chapter then outlines the sections that are to follow: project foundation, business assessment, strategy selection, plan development, testing & maintenance.

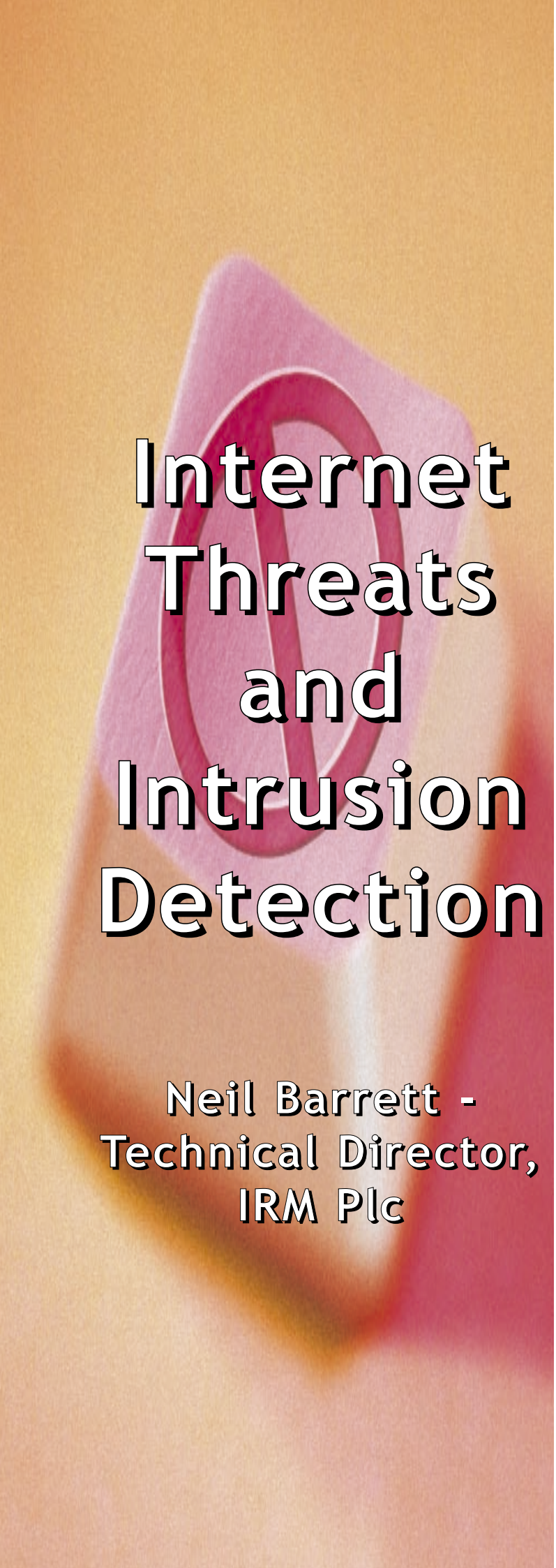
Project foundation discusses the problems of mobilising a project that will usually cross functional boundaries. Business assessment deals primarily and correctly with availability risk. Strategy selection covers the various options available, but also makes it very clear that BCP is more about avoiding problems by building fault tolerant systems than recovering from them. Plan development deals with procedures that will recover an organisation's minimum production capabilities and emphasises that the DRP component must be 'executable, testable and maintainable'. Testing & maintenance addresses the problems of testing in an e-commerce environment and makes the point that incremental and fairly continuous testing is required. The book is well structured and because it is project based provides a logical and comprehensive guide to the subject.

However, the book has the little 'e' letter in its title, so I immediately started looking for those aspects of BCP that are specific to e-commerce. As e-commerce is frequently an extension of bricks and mortar commerce I anticipated a great deal of overlap between the two which is exactly what I found, but I also expected the specific e-commerce problems to be defined and discussed. Although there is a reference to the importance of supply chain logistics for retail operations when operating in a B2C/B2B environment, there is much less than I would have liked. The real problem with BCP in an e-commerce environment is the multitude of partners involved in even the simplest process. This is raised as a concern, but the need for the BCP to cover the business partners as well as one's own company, receives very little treatment.

Basically, BCP has two main components: firstly, prevention of adverse circumstances that would stop the business from functioning and secondly, correction (disaster recovery) to get the show back on the road when the prevention mechanism fails. The authors quite rightly separate the two aspects and comment that 'the focus needs to be not on recovery planning, but on availability planning', however a great deal of this book is about traditional DRP, rather than the effort that must be made to keep the show on the road. During the London Blitz in World War Two, a British theatre, The Windmill, had the slogan 'we never close'. This is exactly what e-commerce is all about: remaining open no matter what the problem encountered. The elimination of single points of failure by using duplicate and triplicate components, automatic switching between these and early warning indicators that identify problems before they become fatal are the real name of the game.

Ultimately this book is about motherhood and apple pie. It is a useful book for anyone wanting a useful guide to disaster recovery, but that is not the same as business continuity. I am also unsure as to its intended audience. According to the disclaimer at the beginning it was designed 'primarily as an educational resource for control professionals'. If this refers to auditors, then the references to CobiT are somewhat thinner than I would like. The audit programme in an appendix does refer to the CobiT Delivery and Support modules, albeit at a high level, but I cannot agree that it 'highlights those special requirements of e-commerce' which is claimed at its introduction. If the target audience is management, then more detailed references to the use of international standards, such as ISO 17799, would have been a useful addition.

If you need a general guide to BCP, then this is a suitable text, but the magic 'e' letter in the title sets an expectation that is not really delivered. We have been dealing with fault tolerant systems for years, that's how the nuclear industry works, so why should e-commerce be that much different?



Internet Threats and Intrusion Detection

Neil Barrett - Technical Director, IRM Plc

The Internet is a source of tremendous benefit for companies, but equally a source of significant threats. Any company using the Internet within their business operations - to sell or market on line; to communicate with customers, suppliers or staff; or simply as a source of relevant information - must address those issues.

The Internet is used by computer hackers, by fraudsters, by pornographers; it contains viruses, illicit copies of applications and of copyright-protected music; and it can be used by people to threaten one another, to abuse one another, or simply as a time-wasting recreational ground. All of these elements need to be considered, policed and reacted to appropriately… But perhaps the most significant of the threats come from that collection of individuals and loose groups that we call 'Hackers.' The word 'Hacker' has had many meanings over the years. Originally, it was a term of respect, coined by the young programmers at MIT for those able to create the most elegant programs, and then for those who knew the most about the computer systems upon which the programs were run. A series of newspaper articles in the US, however, popularised the use of the word to describe those who subverted security on computer systems - and it is this meaning, more or less, that has stuck.

A good working definition for the word would be 'one who does things that would be contrary to the 1990 Computer Misuse Act or similar laws in other countries.' In other words, one who breaks into computers, creates computer viruses, blocks access to systems or networks, etc, etc.

There are many different types of hackers. The most numerous are those that are disparagingly called 'Script Kids': usually adolescent males who take copies of hacking utilities, without necessarily understanding them, and who apply the utilities against a variety of computer systems. They are usually unfocused, unmotivated and random in their activities; their objective is often either to show off to their friends or to collect a number of different types of victim. They cause problems because of their clumsiness, but can be addressed simply by ensuring that computer systems are not left in a state where they are vulnerable to the common hacking utilities. Script kids will not persist in their attacks against an apparently protected computer system, but will instead move on to attack alternative targets.

By ensuring that computer systems are not vulnerable to the common weaknesses exploited by these script kids, the vast majority of the 'hacking problem' can be resolved. A simple programme of system patching and maintenance solves almost all problems.

There are, however, more professional, more determined, and more knowledgeable hackers that must also be considered. Although there are professional hackers, working usually indirectly for

corporate intelligence services, by far the greatest risk from the determined attacker arises from a company's own employees - either current or recently departed. These are the people who know most about the systems; these are the people that are already, to a greater or lesser extent, trusted to access the computers; and these are the people who might have the greatest reason to wish to damage the company. They know what information is most valuable; they know how to benefit from access to that information; and they might well be disgruntled and motivated because of the company's actions towards them.

Obviously, any protection and monitoring system must consider these individuals to be the greatest threat - an ironic observation, given that the computer security industry has spent many years developing and marketing technologies, tools and techniques to protect against the external attacker. The types of attack can equally be considered to form a range. Perhaps the most obvious types of attack associated with computer hacks are intrusions, in which access is gained to one or more computer system within a network. Problems can equally be caused, though, even if the hacker does not gain access, if they can prevent others from gaining access. These flooding or 'Denial of Service' attacks are a particular nuisance because the attacker can hide very effectively, and many of the common ways of providing network security - such as firewalls - are essentially useless against such attack.

The aim of most hackers, however, is still to gain access in preference to blocking access for others. For the purposes of analysis, it is normal to divide these intrusion attacks into two categories: web site intrusions, and gateway intrusions.

Web site intrusions are perhaps the most apparent types of hacking attack: they are, after all, immediately apparent. Access is gained to a web server and some simple alteration to the pages is made. In most cases, the initial, index page of the web site is replaced by the hacker's uploaded page. This might be a simple alteration of the original, or it might be an abusive, pornographic or even amusing content. In a gateway intrusion, by contrast, access is gained to the entire corporate network through the company's Internet gateway - usually separate from the web site itself, which is often hosted by a different company.

Gateway intrusions are less publicly obvious and considerably more damaging for the victims: in these attacks, the intruder has gained access to the entire range of information resources relied upon by the company. They can create untold problems for the organisation … but equally, such intrusions are substantially more difficult to achieve, and are therefore more often associated with professional hackers or with rogue employees.

The actual hacks themselves then fall into two distinct categories: system- or service-level exploits, and application vulnerabilities.

A computer system connected to a network provides a number of distinct services over that link, each associated with a different 'port' on the network. The best analogy is with a large building on the street: the street is the network link, and the different doors and entry points into the building are the different ports. Each entry point might be used for a different purpose - staff entry, good inward, etc - and be used in a different way. Within the computer, each service is represented by a so-called 'daemon' process: a program that can be accessed remotely and which will provide a link to the main service utility. Different computers will support different daemon services connecting to the network through different, usually standard ports. Web services, for example, are usually provided over port 80, electronic mail over port 25, etc.

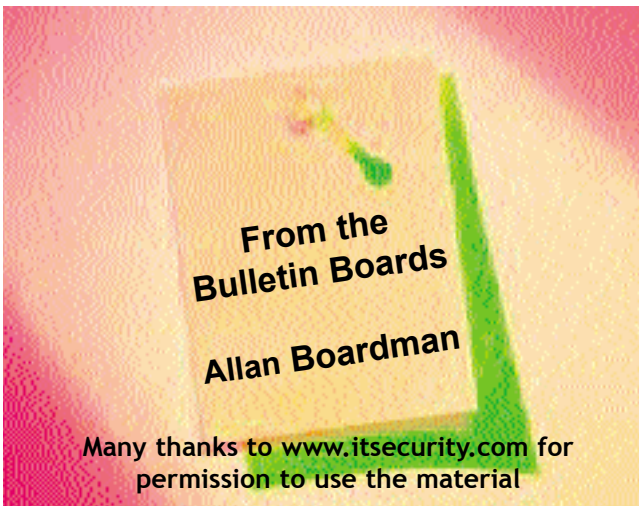
These daemon services might well have known weaknesses and vulnerabilities, allowing an attacker to subvert them using a hacking tool. For example, old implementations of a particularly popular file transfer program have a vulnerability that can be trivially exploited so as to gain remote, highly privileged access to the computer system.

These types of vulnerability can be addressed by ensuring that the version of the daemon or utility is kept up to date: that patches and alterations provided by the supplier are routinely applied, so as to ensure that any newly discovered opportunities are quickly removed. In addition, security technology - such as the now ubiquitous firewall platforms - protect these potentially vulnerable services by ensuring that no harmful elements of network traffic can be launched against the particular port concerned.

As individual services become increasingly well-protected, attention has then shifted to the alternative form of attack: application-level vulnerabilities. These vulnerabilities exist where a secure service has been implemented, but its use is not secure. The most obvious would be passwords: the actual mechanism of protecting a system through passwords is well understood and secure, but if the user chooses a trivial password then it is equally trivially breached.

Application-level vulnerabilities are increasingly a problem for web services. The actual computer running the web service can be highly secure: with no services other than the web traffic itself operating; with the web service patched and well-maintained so as to leave no service-level opportunities … but with the implementation of the web pages vulnerable. For example, a web application that examines a back-end database - using standard queries constructed using SQL - might

Continued on page 27



Question:

With the implementation of the Human Rights Act 1998 into UK law, what is the generally held view on interception of employee e-mails? Article 8 states that "Everyone has the right to respect for his private and family life, his home and his correspondence." If you are not investigating a case of fraud, harassment etc., how would you stand if an employee levelled an accusation of violating this article, if they discovered that e-mail interception was taking place? I think that everyone would sit up and take notice, if their employer had the rights to open any envelope that was sent through there internal snail mail system. Why is an e-mail any different in that case?

http://www.itsecurity.com/asktecs/nov4202.htm

Response from Robert Schifreen, Information Security Training Ltd

The generally accepted view in the UK is that it's OK to monitor employee email that is sent or received for business purposes, but you should always tell employees (and recipients of messages) that you do it.

As for personal email, some companies simply ban all personal email. Others allow it, but point out that the company monitors it. Others provide a separate PC, not linked to the LAN, that staff can use to send and receive unmonitored personal email.

You're right, that monitoring personal email (even with permission) may be in conflict with human rights laws, but there's not been a test case yet as far as I know. So you should be OK if you do it.

In other countries, it varies. In Germany, for example, it's definitely illegal to monitor personal email so many companies simply ban it outright. Any message is thus assumed not to be personal, and can therefore be monitored.

Response from Mark Smith, Morgan Cole

I think the first point to note is that the Human Rights Act ("HRA") applies directly to public bodies and those exercising public functions. While there is some debate among the legal community that it will have a wider effect, this is far from certain at present.

The second point to note is that the one consistent theme running through the majority of the law in this area (Lawful Business Practice Regulations & RIP Act, Data Protection etc) is that employers need to tell their employees. If they have done so and their policy and practice complies with this legislation, is responsible and enforced consistently, and ensures that employees clearly understand what their expectations of privacy should be, it is unlikely that the HRA would cause additional complications.

Response from Dancho Danchev, Frame4 Security Systems

No matter what the law says in any particular case, you can never be 100% sure that someone isn't intercepting your e-mails as soon as you're sending them in plain text, which is the way I'm sure you do. No matter what someone tell you, trust only yourself. Encrypt your messages using PGP, but if you're not familiar with it, zip and password protect the e-mails and send them as an attachment, just be adaptive and never send confidential or personal information in plain text. I also recommend you to take a look at http://www.hushmail.com which is a service I'm sure you'll start using.

Response from Barry Mattacott, e92plus

It should be stated in your employment contract that your management reserves the right to monitor your email. In which case you signed on the dotted line and accepted it. There should be no "finding out" about it as it must be declared up front. The key point is that you are using your employer's resources (email system) for your personal use!

Response from David Grant, Halcrow Group Ltd

The Human Rights Act (1998) , the Lawful Business Practice Regulations 2000 (made under the Regulation of Investigatory Powers Act 2000) all have an input in the monitoring legislation. Under all of this legislation, the Acceptable Use Policy (AUP) is stating that Internet and or e-mail will be monitored and explaining the reasons for that monitoring, and that the User has agreed to this policy will cover the requirements of this

legislation. A note of caution should be added here. The law in this area is too recent to have established precedents. Employers need to consider this when defining the scope of personal use of business facilities and the configuration of technical solutions to underpin AUPs.

Question:

This is a supplementary query to query # nov4202.

Our company allows personal mail, but states that e-mail interception may take place. What position would you be in though, if you intercepted employee mail, which contained information that was the subject of legal privilege etc?

As for the Human Rights Act, I thought that the interpretation, was that UK courts were considered "a public body", and had a duty of care to see that the articles were upheld even in private organisations. Otherwise private companies could go around exercising powers beyond governmental levels, and I don't believe this to be the case.

I also believe that the RIP Act was brought in to introduce the principals of legality to the police and internal security organisations when they are engaged in covert interception of communications. This local legislation exempts their activities from the Human Rights Act.
If the government introduced legislation to cover itself in this matter, are we all just dancing on a pin-head?

http://www.itsecurity.com/asktecs/nov4402.htm

Response from Robert Schifreen, Information Security Training Ltd

Myunderstanding of the way things work in practice is that, if you warn employees that email is monitored, it's up to them to decide whether they want to risk personal information being seen by the person or program doing the monitoring. If they don't, they tell their friends not to email them at work.

Response from Andrew Odendaal, 4FrontSecurity, Inc.

Companies have the right to interrogate mail - but I would suggest that they must have Security and HR Policy to support this. As for legal privilege, the company's right is protected - it is dependent upon what is in the email and under what context the subject matter is being used for. If this is a problem - I would suggest that anything that affects the rights of the individual should not be done at the workplace, but from a private email address - which could be protected if necessary!

May I suggest that companies do exercise powers beyond what may be considered fair. Organisations are open to attacks from both external and internal sources, they must protect themselves from this. Legislation is being imposed to CEO's and business leader to ensure that risk is mitigated - if it isn't they will be held personally responsible. organisations MUST be in control of their destiny, regardless of legislation. Employees must also be aware that they go to work to earn money and support the company they are employed by! If subversive activities are undertaken (and caught) then the employee must suffer the consequences!

There is an easy answer to this question - we do not know all the activities that are undertaken by the government agencies - the easy answer is YES we are just dancing on pin-heads - the Internet is a dangerous place, you are personally under attack! You are being spied upon! Your information is not yours! Be extremely careful out there!! Remember one other thing - the law is the law - MIGHT IS ALWAYS RIGHT!

Response from Barry Mattacott, e92plus

Welcome to the nightmare!! This area is a minefield and if you don't want to get fragged by a claymore you'll tread lightly.

It is known and documented that certain areas the RIP Act and the Human Rights Act contradict each other and also EU guidelines and laws. I would advise that if you are digging this deep into this area that you should seek specialist legal advice to safeguard both yourself and your enterprise. Although the esteemed Experts of the Security Clinic give great advice on security issues, this is one area that I'd feel more comfortable if I paid for it. At least if anything goes wrong then, you'll have someone to sue!

It makes no difference because all of this is already catered for in the statutory instrument called the Lawful Business Practices Regulations which is an adjunct to the Regulation of Investigatory Powers Act RIPA. Full wording of both of these instruments can be found on the "Her Majesty's Stationary Office" website www.hmso.gov.uk.

Response from Phil Ryan, Security Architect

Basically the regulations make it permissible to monitor email for a wide number of reasons as long as you have told everyone that you are going to do so. There are also a few circumstances which you can monitor covertly but these are far more prescriptive. You may also wish to note that

these regulations certainly apply to telephone communications as well and could easily be interpreted as applying to postal communications. In my opinion if employees wish to have electronic mail for private purposes which they do not want their employers to see then they should get their own connection at home. You would hardly expect an employer to allow it's employees to bring all of their private correspondence into work to use the company franking machine to post them.

Question:

Where can I find a white paper that gives general advice on best practice application coding principals?

http://www.itsecurity.com/asktecs/nov4302.htm

Response from Kevin Townsend, ITsecurity.com

If you do a web search on 'secure coding' you will get literally hundreds of useful links. There is also a range of books that you could look at, including (check Amazon for details):

- Hack Proofing your Web Applications from Syngress.
- Building Secure Software from Addison Wesley.
- Web Security & Commerce from O'Reilly.
- Web Hacking: Attacks and Defense from Addison Wesley
- Developing Secure Applications with Visual Basic, from Sams
- Writing Secure Code, from Microsoft Press
- Secure Programming for Linux and Unix HOWTO, by David A. Wheeler (available free on the web)

The last entry is particularly noteworthy because:

1. it is freely available on the Internet
2. it is maintained by David Wheeler and is consequently more up to date than many alternatives.

It can be found at:

http://dwheeler.com/secure-programs/Secure-Programs-HOWTO.html.

Many thanks to www.itsecurity.com for permission to use the material

We have received two proposals for Special Interest Groups from Cynthia Garibotto a London Chapter member from Price Waterhouse Coopers.

IT Project Auditing SIG

The objective of this SIG is to advance members' knowledge in the field of auditing projects. It would be relevant to Chief Information Officers, Chief Technology Officers, IS Auditors, Internal Auditors, Project Managers, Consultants and other members with a particular interest in the topic.

Some of the proposed deliverables are Audit Guidelines, Presentations, Exchange of ideas and Articles.

If you are interested in helping set up a Project Auditing SIG or would like to be involved with it in any way, or would just like to find out more, please contact Cynthia Garibotto at cgaribot3@yahoo.com

IT Security Awareness SIG

The objective of this proposed SIG is to advance members' knowledge in the field of IT Security Awareness. It would be relevant to Chief Technology Officers, Chief Information Officers, IS Auditors, Security Administrators, Consultants and other members with a particular interest in the topic.

The proposed deliverables are an IT Security Awareness Programme, Presentations, an exchange of ideas, and articles for Datawatch.

If you are interested in helping set up a SIG or would like to be involved with it in any way, or would just like to find out more, please contact Cynthia Garibotto at cgaribot3@yahoo.com

Kamal Khan

Continued from page 23

be vulnerable if no checks have been established on the format of input allowed to the various fields. If a rogue user can introduce SQL commands in place of, say, usernames or passwords then the back-end database can be exploited.

These application level exploits are particularly difficult to prevent. Firewalls are essentially useless under these circumstances: the network traffic is of a permitted form and is being transmitted to a permitted service over a permitted port; the firewall has little or no reason to complain about it … but the application receiving that traffic is being subverted.

Intrusion detection systems were developed, at least in part, to help address these problems. Firewalls act rather like bouncers at a nightclub: they stand at the doorway and try to decide whether someone should be admitted or not. But they guard only what they have been told to guard, and determine admittance or rejection based on the rules that they have been told to apply. By contrast, an IDS is like a store detective working within a shop. The detective can move around, and can concentrate on individuals that might appear only vaguely suspicious until they do something definite; and of course, the detective can allow some limited 'bad things' to happen before then stopping the culprit.

The IDS system has a number of monitoring points within a network, including sensors on the network segments themselves and on the computers connected to the network. Traffic patterns can be considered over quite extensive periods of time, and intelligence gathered from different points of the network can be combined and analysed together. The result is a much finer understanding of the nature of traffic within the network, and a much more reliable way of determining whether that traffic should continue to be permitted or should be prevented.

As an incidental benefit of this approach, the use of IDS also allows traffic coming from insiders to be policed, a task that simple firewalls cannot achieve. The application of an IDS therefore addresses the increasingly popular application-level attacks and polices internal misuse of systems. In many ways, it might be considered an ideal solution to the problems of information security faced by most organisations. There are, however, some problems that must be addressed if IDS is to be well used. Most obviously, IDS sensitivity can result in excessive alarm conditions being raised, and requires a security function to be implemented within the company so as to handle those alarms: staff able to respond and some instructions from senior management as to how they are to respond.

Because of the sensitivity and intelligence of IDS it can handle flooding attacks, intrusions and internal misuse, and it can collect evidence of malicious or criminal activities so as to support a prosecution. Provided that the IDS is therefore seen as a way of supporting reaction staff, it is an ideal way of addressing the most common hacking problems faced by organisations.

It is important to bear in mind, however, that IDS is not the ultimate solution to the problem of information security. It can be used in conjunction with a staff function, with an on-going programme of maintenance and patching, and with continuous monitoring of employee activity. There is no 'Royal Road' to information security, and it is vitally important always to bear in mind the most important observation of all:

Information security is a process and not a property.

Neil Barrett, Technical Director, IRM PLC

Information Risk Management plc (IRM) provides all forms of Information Security services, including Penetration Testing, Computer Forensics, Incident Response and Consultancy. A market leader in computer security, IRM uses a 'scenario based' methodology that can be tailored to each client's needs, rather than 'one size fits all' approach favoured by many in the industry, and is independent of any security product vendor. IRM has a client list including many of the FTSE 100 as well as top companies from across the globe.

If you would like to know more or would like to speak in confidence to one of IRM's consultants regarding any security issue please do not hesitate to call 020 7808 6420 or email them at enquires@irmplc.com

IRM plc
22 Buckingham Gate
London
SW1E 6LB

INTERNET RESOURCE LIST

AUDIT

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

SECURITY

www.cert.org
ciac.llnl.gov/ciac/
spam.abuse.net
www.cl.cam.ac.uk/spam/
www.iki.fi/liw/mailfilter.html
csrc.nist.gov/secpubs/unix_security_checklist.txt
www/ntsecurity.net/
www.first.org
www.cauce.org/
http://www.securityportal.com/
http://www.antionline.com/
http://www.cerias.purdue.edu/coast/hotlist/
http://www.sse.ie/securitynews.html
http://www.infosyssec.org/infosyssec/index.html
http://web.mit.edu/security/www/gassp1.html
www.eSecurityOnline.com
http://www.pki-page.org/
http://www.microsoft.com/TechNet/win2000/win2ksrv/prodfact/pkiintro.asp
http://www.sans.org/topten.htm
www.securitywatch.com

COMPUTER COMPANIES AND SYSTEMS

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

OTHER ORGANISATIONS

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

HACKERS AND VIRUSES

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

AREAS OF AUDIT INTEREST

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