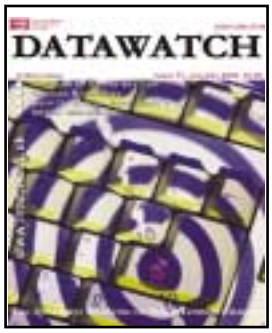
51, Jan-Apr 2002

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

plus: All you need to know about CISSP on page 18

ISACA London Chapter Committee 2001/2002

PRESIDENT
Karen Sharpe
TXU Europe
01473 554172
karen.sharpe@txu-europe.com

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CHAPTER OFFICE
Nancy Watt
01487 815705
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

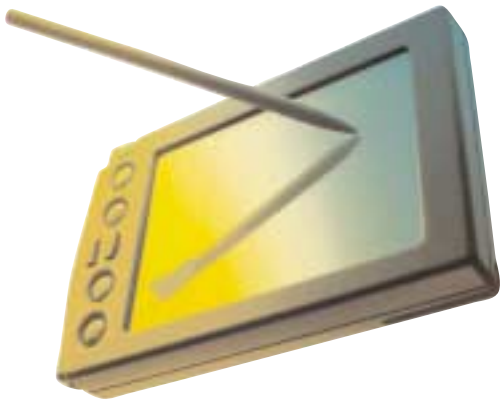
SECRETARY
Chris Chandler
Arthur Andersen
0121 233 2101

TREASURER
Geoff Adey
KPMG
0121 232 3202

PAST PRESIDENT
James Whittaker
BT
0121 230 2214

WEBSITE:

www.isaca.org.uk/central



Hello and welcome to another edition of Datawatch! I hope that you all had a good Christmas break and a good start to 2002.

We have a range of articles for you this month covering several topics. Martin Gordon of Defcom has written a technical article on IDS - that's Intrusion Detection Systems for those of you who don't use TLAs (Three Letter Acronyms).

There is an article on the Basel (Capital Adequacy) Accord on IT and risk management systems by Amgad Kamel, which should be of interest to those of you who work in the banking industry and Simon Moore of BDO Stoy Hayward takes us Back to Basics on using CAAT's.

Ever thought of taking another qualification? Brian Shorten has submitted an article on the CISSP qualification (Certified Information Security Systems Professional) which those of you who specialise in the more technical aspects of IS auditing or in IS security itself may well find useful and/or complementary to CISA. I didn't know much about it before but Brian's article has certainly made me think about its usefulness.

There are of course your regulars on Security, Netwatch, the Bulleting Boards and recruitment, in which Adrian Simpson talks about the demand for computer auditors - something of great interest to us all! We also introduce the first in a series of articles, "Software Spotlight" by John Mitchell.

I was reminded the other day that CPE points - those elusive things we all try to build - especially when next year's membership demands land on our desks with the request to fill in our hours for this year - are available for attending Chapter meetings and for contributing to Datawatch. So there's yet another reason for writing an article for this award winning magazine!

ISACA London Chapter Programme of Events 2001/2002

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

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

Thursday 22 November 2001
Selling Your Recommendations
Lindsay Mercer
BAA

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

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

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

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

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

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

Thursday 27 June 2002
Desktop Audit
TBA

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

MIND GAMES

Find the following words in the wordsquare below. Once all the words have been located, you will be left with 8 "unchecked" letters. Unscramble these to form an Audit-related word. Words may be forwards, backwards, vertical, horizontal or diagonal.

RESOURCE, AUDITOR, E-BUSINESS, ISACA, FORENSIC, RECRUIT, INVENTORY, SIREN, ABOUT, STUPOR, TRADER, ROLLING, MEADOWS, ORDER, CRASHED, ASIDES, SOLID, BREWED, CARRIER, SHAME

Answers on page 28.

I	N	V	E	N	T	O	R	Y	C
S	E	D	I	S	A	C	E	U	I
W	R	E	S	O	U	R	C	E	S
O	I	H	R	E	D	A	R	T	N
D	S	S	E	N	I	S	U	B	E
E	M	A	H	S	T	P	I	R	R
A	E	R	A	B	O	U	T	E	O
M	T	C	I	R	R	L	D	W	F
C	A	R	R	I	E	R	I	E	S

FROM THE PRESIDENT

I started a new job in November 2001. In some ways, it's more than a new job; it's another change in the direction of my career. I am no longer an IT auditor, nor an auditor of any description for that matter. I am now a Financial Controller, responsible for working capital management in a large, American owned company in the energy sector.

I can hear people thinking, as I confess I did to myself at first, so what use is ISACA and the hard work done to achieve CISA certification now? Well, it has quickly become apparent to me that I need to use a considerable amount of the knowledge that I have gained as an IT auditor in my new role. I now find that I am one of the key business users on two major systems implementations. I am also responsible for a considerable amount of data that needs to be cleaned up prior to migration, which has resulted in my being project sponsor of a number of sub-projects. Even with existing systems, I am asked to consider and approve change requests that may have an impact on my team's data. In addition, like many finance teams, mine uses a bewildering array of complex and interdependent spreadsheets - it's early days for me yet, but I am prepared to put money on them not being well controlled! I could go on, but I think the point is made! Membership of ISACA continues to be a valuable addition to my personal "tool kit" of knowledge resources.

If I go back to when I first emerged as a newly qualified Chartered Accountant, I felt that I needed more knowledge about IT and its control if I was to be a successful external auditor. That was the point at which I turned to ISACA for more knowledge. What has happened to me since has convinced me that I was right. It is becoming increasingly difficult for business managers to remain ignorant of IT controls and governance issues. IT systems are completely embedded in most companies now and we rely on them to survive from day to day and carry out all business critical functions. Managers and, dare I say it, Executives, cannot afford to allow themselves the luxury of being unfamiliar with their business critical IT systems.

None of what I have said so far is news to anyone and many business managers have recognised the importance of IT and sought to improve their own knowledge through means other than ISACA. However, that does not detract from ISACA's own success at providing the right education, certification and research opportunities. During my interview process, my new employers had not heard of ISACA or CISA, but when I explained what CISA meant, they were very impressed and told me that they thought these skills would be useful to me in my new environment. This in itself answers my own question above - the hard work in becoming a CISA was worth it, particularly in terms of enhancing my own career choices.

For those of you who are considering sitting CISA in 2002, the registration forms need to be completed and submitted soon. Early registration, which attracts a reduction in cost, closes on 13 February 2002 and final registration is 3 April 2002. Don't miss those dates, or you will have to wait an extra year to become CISA certified and experience the resultant benefits.

Now is also a good time to think about your training programme for 2002, particularly for existing CISAs who need to maintain their qualification through continuing education. The two main ISACA conferences for European members are the EuroCACS Conference, taking place in Budapest, Hungary from 24 - 27 March 2002 and the International Conference, which is in New York, USA from 7 - 10 July 2002. On a smaller scale, don't forget that the London Chapter hosts a one-hour educational event on the fourth Thursday, followed by a networking and discussion opportunity. We also try to put on one-day training events during the year, when there is sufficient interest from our membership to enable us to do so. Details of all of these sessions can be found on our website.

If anyone should wish to become more involved in ISACA, or to "put something back" into the profession, there are plenty of opportunities available, ranging from becoming a CISA mentor to becoming a local or international Board member. Just contact me, Nancy, or indeed any other member of the London Chapter Board, for more information.

With that, all that is left is for me to wish you a Happy New Year and success in your endeavours in 2002!

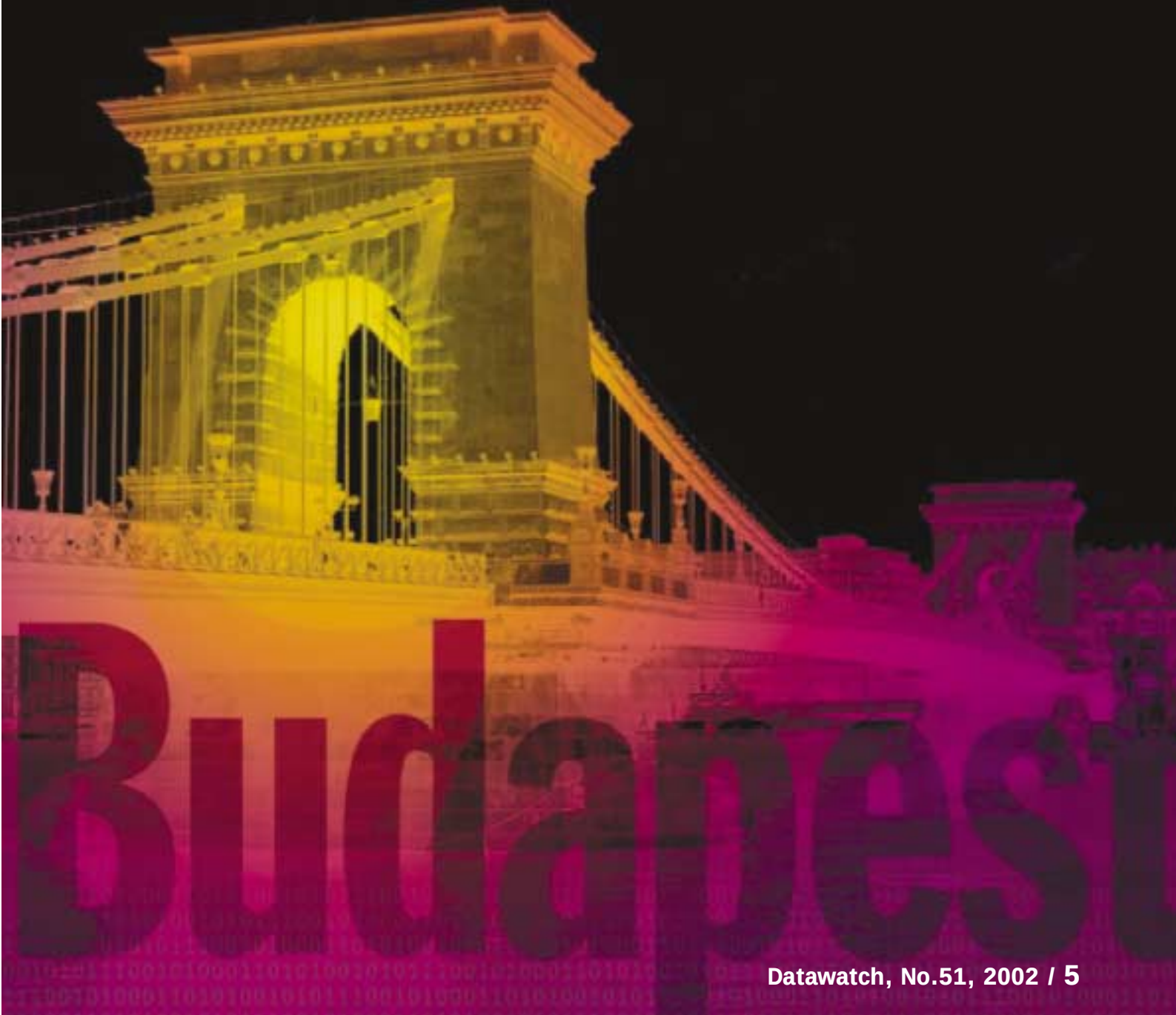
Karen

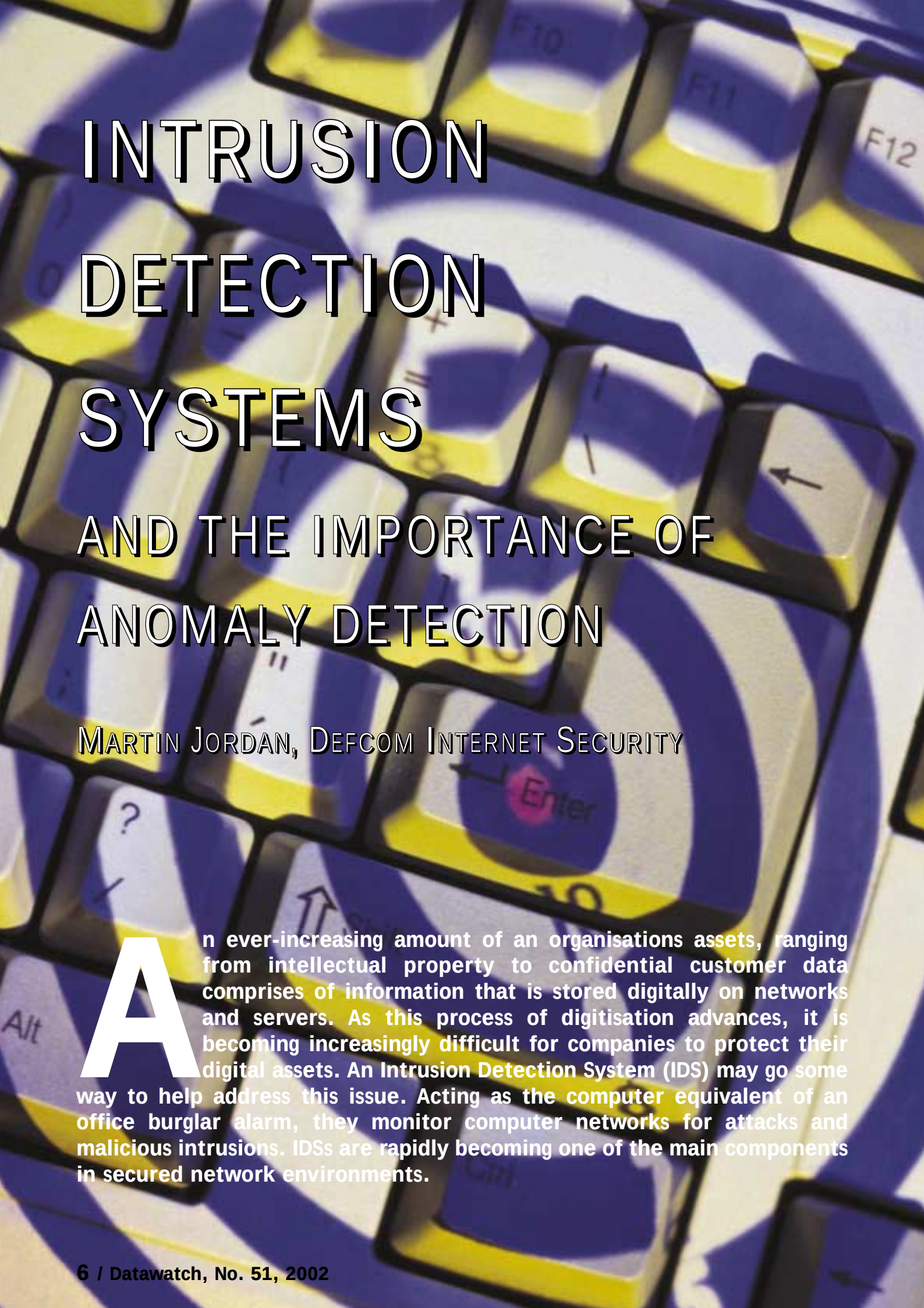
EuroCACS 2002
24-27 March 2002
Hotel Intercontinental Budapest
Budapest, Hungary

For Conference Information:
Web site: www.isaca.org/eurocacs2002.htm
E-mail: conference@isaca.org
Call: +1.847.253.1545, ext. 485

euro cacs

EuroCACS 2002 is presented by Information Systems Audit and Control Association®





INTRUSION DETECTION SYSTEMS

AND THE IMPORTANCE OF ANOMALY DETECTION

MARTIN JORDAN, DEFCOM INTERNET SECURITY

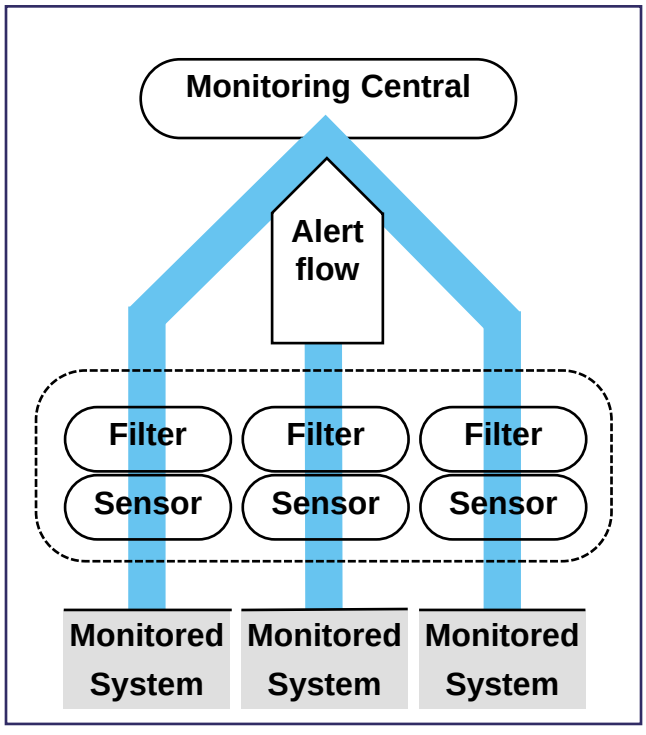
An ever-increasing amount of an organisations assets, ranging from intellectual property to confidential customer data comprises of information that is stored digitally on networks and servers. As this process of digitisation advances, it is becoming increasingly difficult for companies to protect their digital assets. An Intrusion Detection System (IDS) may go some way to help address this issue. Acting as the computer equivalent of an office burglar alarm, they monitor computer networks for attacks and malicious intrusions. IDSs are rapidly becoming one of the main components in secured network environments.

Intrusion Detection Systems are monitoring programs aimed at detecting 'intruders' who are acting 'illegally' in a computer system. The significance of 'intruder' and 'illegal' depends on the limits set by a security model, but can be generally defined as a person or process performing unauthorized operations on a network element (server, router, workstation...) in an attempt to gain more control over it.

An IDS comprises of 4 distinct successive layers: a sensor, running some filters that are generating an alert-flow directed to a monitoring central. For this article I have focused upon the most important parts of an IDS, filters and alert-flow.

There are two main categories of IDSs: host based (HIDS) and network based (NIDS). A host based IDS runs as a process on a host computer and monitors sensitive activities on this computer, such as unauthorized access or modification of files. A network based IDS consists of a sniffer program listening to the network traffic in an attempt to detect suspicious activity on a network. Both host and network based IDSs will generate alarms if they detect suspicious activity. These alarms should trigger a response from the network administrator or some automated response tool. A host based IDS will usually be located on critical computers such as servers, while a network based IDS should be located at strategic points in a network, in order to have access to relevant traffic.

An IDS, whether it is host or network based, usually consists in 4 distinct successive layers: a sensor, running some filters that are generating an alert-flow directed to a monitoring central, as illustrated on figure 1. This general model can be used to describe HIDSs and NIDSs or even Distributed IDSs (DIDSs).



The sensor is responsible for gathering relevant data from the system that is being monitored. The filters are specialised programs checking the data provided by a sensor in order to detect possible attack patterns. Suspect patterns trigger the filters into sending alerts. The alerts produced by all the filters are gathered into an alert-flow. This alert-flow is then directed to a central monitoring station. At this stage, an administrator monitors and interprets the alert-flow and takes the appropriate action.

The efficiency of an IDS depends highly upon on the quality of its filters, since they are doing the actual intrusion detection work. The design and configuration of these filters is a crucial issue when purchasing an IDS. There are a few ways for a filter to detect attack signs inside the data stream provided by the sensor, signature based and anomaly based.

Signature Filter

Signature filters are the simplest and most widespread type of filter. A signature filter basically looks for one specific signature in the data flow provided by a sensor. An attack usually possesses some kind of signature that identifies it. This signature often consists in one or more specific binary pattern found in a given file or network packet.

Although simple to implement, signature filters have a number of limitations. They are able to recognize an attack only when they 'know' a signature for this attack, and thus require continuous updates of their signature database as well as continuous research work to analyse new attacks and find their signatures. Moreover, a slight change in the attack scenario may be enough to alter the attack signature and thus fool a signature filter.

Another limitation is that the process of discovering signatures is complex and unreliable. It relies on an individual having both detailed access to attack logs and the technical skills to analyse them, or who gets to learn how a new attack works. This person should then inform competent authorities of his findings. These authorities then propagate the information among security professionals including those in charge of updating IDSs filters and signatures, manufactures or your managed security provider. Hence, signature filters will not detect attacks until they have been widely discovered, and probably widely used.

Protocol Anomaly Filter

The term 'anomaly filter' is often used to refer to two different kinds of filters defined here as protocol anomaly and statistical anomaly filters.

A protocol anomaly filter is a filter looking for protocol misusage. 'Protocol' should here be

interpreted as any official set of rules describing the interaction between elements in a computer system. A protocol anomaly filter is consequently designed to analyze specifically one protocol, and requires a model of this protocol's 'normal' usage. Protocols always have a theoretical usage, corresponding to their official description in documents such as RFCs2, but experience shows that they are seldom implemented andused in complete accordance with these official descriptions.

A model for a protocols 'normal' usage can thus be defined as the superposition of the official and practical area of usage of this protocol. Any use of this protocol outside these intersected areas can be considered as a protocol anomaly. Experience shows that the majority of the attacks can be considered as protocol usage anomalies. The reason lies in the fact that most of the attacks are exploiting breaches in badly defined areas of protocols, in which special cases have been neglected in the protocol standard itself as well as in its implementations. Protocol anomaly filters are thus able to detect all attacks that are using protocols outside of their normal usage area, which includes in particular new attacks that may not yet have been registered by computer security authorities. This ability of detecting new attacks, added to the fact that they don't require signature database updates and have the same comparatively long lifetime as the protocol they are monitoring, asserts the superiority of protocol anomaly filters over signature filters.

When running above a network based sensor, protocol anomaly filters would disassemble the data packets for each network protocol, and check if they are built in compliance with the protocol standards, as described in RFCs or equivalents. The common implementations of these protocols should also be studied, in order to define the limits of what is officially and unofficially the standard for this protocol. An example of protocol anomaly is to give an extra large username (many kilobytes) with the USER command of the FTP protocol while logging onto a FTP server. Though extra large arguments are not often considered in official protocol standards as explicitly illicit, they should be considered in practice as a suspicious sign, since they are not justified by normal usage and may be an attempt to exploit buffer overflows or denial of service.

A statistical anomaly filter is designed to monitor a system and detect statistically exceptional events. The idea is to build a model of a system's normal behavior under safeconditions, and then to periodically compare the system's behavior against this model. If the difference exceeds some limit, an alert is generated. Protocol anomaly filter can be considered as a special case of statistical anomaly filter applied to a protocol syntax. In a network based context, the behavior monitored could be a user's activity over the network, or a protocol traffic. The model for a normal behavior would be obtained by sampling the corresponding behavior under a period of time representative of safe activity. The same parameters would then be sampled again on a regular basis, and the result compared with the reference model. In a host-based context, the behavior monitored would be more focused on user activities, program activities, file and device accesses, etc. How definitive a reference model should be is a source of dilemma. Indeed, systems behaviors tend to change with time, and statistical anomaly filters should consequently be designed to allow regular updates of their reference model. On the other hand, if this model is updated too often, an intruder could spread his activity over a period of time long enough to let the filter 'learn' his behavior and accept it in its model as a normal behavior.

Another approach to attack detection is to use neural networks to detect attack patterns inside a stream of system information. The idea is to select representative information streams coming from sensors and to connect them to a neural network. The neural network is then 'taught' to recognize specific attack patterns while the attacks are simulated on the monitored system. While elegant in their transparency and flexibility, neural networks present the drawback of not being accurate in pattern recognition: they can hardly ever offer 100% detection accuracy, and thus should not be used as a main filtering technique in an IDS. They can on the other hand be used as a parallel tool helping to confirm attack diagnosis.

Alert-Flow

Another issue in filter design is the generation of alert messages to acknowledge the anomaly or attack detected. This can be divided into two areas: defining a standard for an alert format, and increasing alert accuracy through internal filter programming techniques:

Alert format

Defining an efficient format for alerts is required in order to give accurate information to the human end-user of the IDS as well as to enable alert manipulation by intermediate programs managing the alert-flow. There is currently no standard format for describing alerts, despite the many suggested candidates. Typical solutions involve using general description languages such as XML, or defining proprietary format based for example on key-value pairs. A difficulty is to define a standard flexible enough to be able to describe new attacks, but structured enough to enable automated analysis of its messages. The IETF is about to release a RFC describing a format called The Intrusion Detection Exchange Protocol (IDXP), IETF that is believed to become the alert standard.

With a theoretically perfect filter, each alert sent

would exactly correspond to a real attack. In practice, a filter can often miss an attack or on the other hand send an alert while no attack is perpetrated. An alert of this second kind is called false-positive and occurs typically when a filter interprets some legitimate activity as revealing an attack. Reducing the amount of false-positives is one of the main issues in IDS design.

Filter design for alert-flow control

There are two criteria that a filter should match to provide efficient alert generation:

- Avoid false-positives
- One attack should not trigger a flood of alerts

These two measures aim at reducing the alert-flow and increasing alert relevancy. These requirements can be met by using filter components processing the alert-flow itself. Such a component can be added inside the filter, and works as follow: when the attack detection component of the filter generates an alert, it stores it temporarily in an alert log which is parsed and emptied periodically by an alert filter component. This component analyses the alert log and can:

- Simply forward relevant alerts
- Build a macro-alert summarizing multiple related alerts
- Apply alert level filtering rules to implement a higher level of attack analysis

A filter needs to be customized to fit the system it is monitoring. From a general point of view, the more information a filter possesses concerning the system it is monitoring, the more accurate its analysis can get. Special care is required to design highly configurable filters that can be accurately adapted to a specific system. Their configuration should be easy to do and modify, if possible through appropriate user interfaces. Besides, if filters require periodic manual configuration, they might create a huge work load. An interesting but not yet explored technique to override this problem of periodic filter configuration is to use self-configurable filters. The idea is to design the filters in such a way that they can learn from the system they are monitoring the information that they require to analyse it efficiently. This would especially apply to anomaly filters. Yet, it is likely that some information would still have to be given manually.

IDS filters generate an alert-flow, which is ultimately directed to an end-user, whether it is an individual or an automated response tool. For this end-user, monitoring and interpreting the alert-flow is a complex task that can be made simpler by inserting alert-flow preprocessing components between the filters and the end-user. Most actual IDSs do not offer simple alert-flow preprocessing.

In the simplest case of IDS, alerts are just stored in a log file and it is up to the end-user to analyse it properly. To facilitate this task for the human end-user, most modern IDSs provide a (Graphical) User Interface to the alert-flow. The design of such an interface is an important issue, since its purpose is to help the end-user to analyse the raw alert-flow generated by the IDS. An in-depth analysis of IDS GUIs' requirements is beyond the scope of this document, but we can list a few common features that they should possess:

- They should be designed in order to clearly show important alert information, such as IP addresses and alert type and severity.
- They should help in sorting alert by severity.
- They should provide information on what the alert means.
- They should possess some customizable filtering capabilities, to filter irrelevant alerts.

Alert Storage

All alerts generated by the IDS should be stored permanently for later inspection in a dedicated database, in order to facilitate post-attack analysis and forensics. A database is preferable to a raw log file, since it is more adapted to automated report generation and query work. This database should be secured, preferably located on a dedicated computer, isolated from the monitored network and connected to the IDS through a separate channel. Alerts could be stored encrypted.

Summary

While computer systems are invading every corner of our lives and getting complex and hard to secure, the knowledge of how to exploit their vulnerabilities is simultaneously reaching more and more users. Intrusion Detection Systems (IDSs) are playing an increasingly important role as a security component to build secured network environments. After about 15 years of development, IDSs are now starting to be available on a large scale. Yet, there remain a few obstacles that current IDS technologies are still unable to address. The near future of IDSs will mainly depend on their ability to find solutions to these challenges.

Defcom Internet Security offer 24x7 Managed Intrusion Detection from offices in London and Stockholm. For further information please contact Martin Jordan on 07900 408 760 or at martin.Jordan@defcom.com

Question:

What do you consider to be the greatest security risks to organisations in 2002?
(http://www.itsecurity.com/asktecs/sep3301.htm)

Response from Iain Franklin, Entercept Security Technologies

I perceive that one of the greatest risks in 2002 will be the continued development of new worm technologies targeted at critical Servers. Over the last few months we have seen a monumental change in hacking activity. With the emergence of the Code Red worm, hackers have discovered a whole new way to cause mass destruction in a minimum amount of time. After the onslaught of Code Red we have seen revised and more malicious versions of the same worm technology causing destruction worldwide. Code Red V2, Code Blue, and more recently the Nimda worm have exploited more, and different, vulnerabilities but are essentially all spawns of the same original code but getting cleverer with each mutation.

Now that hackers understand how to write reliable worm code, we predict that we will see an influx of these types of attacks on Internet facing servers. We foresee these worms defacing sites, bringing down entire company's servers and attempting to slow down the Internet. The worrying thing about attacks directed at server level is the mission critical data that is stored on them which could be easily exploited in several different ways. During the next year we expect to see worms directed not just at Microsoft's IIS but, as hackers get to grips with modifying code, other servers such as Apache and iPlanet targeted too.

We envisage many variations of worm technology attacks throughout 2002 and beyond until people become aware of the need for dedicated server protection. Preventative technologies, which will protect a web server even if the latest patches have not been deployed, are already available but there is a need for education about, and more widespread take-up of these solutions before we will see the back of this type of attack.

Response from Ted Doty, OKENA

The greatest security risks facing organisations in the next year will be the same risks that have faced organisations for quite some time -- the new attack that hasn't been defined or planned for that could potentially cripple desktops and networks until an appropriate "patch" or downloadable solution is available. IT loses twice in this situation - First, they spend a huge amount of effort chasing the "patch du jour" or adding new signatures to security devices, rather than adding new services or improving service levels. Second, even if they step up to the expense and headache of this patch management nightmare, there will always be a window of vulnerability during an attack, when no patch or signature exists. It's during this window that some of the worst damage occurs - system outages, data loss, servers that have to be rebuilt.

Consequently, it's critically important that IT tries to get ahead of the game, by finding ways to implement proactive security solutions. Preventing damage from occurring in the first place - even with new attacks that we've never seen before - is the only way to regain control of their time. Reactive security technologies have been with us for years, and the track record shows that administrators can never get out of the update race. The only efficient way of dealing with unanticipated security risks is to prevent them from executing their malicious code - defining appropriate application behaviour and enforcing that behaviour. When applications are prevented from behaving in ways that are counterproductive and not in line with their true functions, only then will the enterprise infrastructure be truly safe from damage associated with crippled systems.

Response from Chris Cook, Security Awareness Inc.

One of the biggest risks we see continues to be a lack of user awareness. The best networks, firewalls, VPNs and the like can all be rendered useless by one careless or uneducated user. All of our lives our parents, friends, society and human nature teach us to be helpful to others. It's ingrained in most of us. Hackers, social engineers and now, even virus authors are praying on this human trait as a weakness. Effective and continued security awareness training should be a priority within most organisations. Their people are often the last line of defence in protecting information resources and assets.

Question:

We're hearing a lot of rumours and reports that terrorists are using steganography rather than cryptography. What is steganography? How does it work? Why would anyone use it instead of encryption?
(http://www.itsecurity.com/asktecs/oct2301.htm)

Response from Sarah Carter, HarrierZeuros Ltd

Steganography is the practice of hiding information in computer pictures or music and relies on the fact that digital images and MP3 music files are made up of thousands of pieces of binary code, which tell a computer to colour a pixel or produce a sound. Because so many small pieces of digital information are involved, a handful can easily be altered to convey secret messages, without changing the overall effect to the naked eye or ear.

Normally, the secret information is stored in the least significant parts of an image or tune. In a holiday photo, for example, dozens of pixels in the background could be changed to convey an airline schedule. To a casual observer, or even an FBI investigator, the picture would appear completely innocent, as the vast majority of the pixels are not changed. Anyone who knew where to look, however, would be able to access the information hidden in the altered pixels, which can then be pieced together and read as normal. It is a relatively simple practice and can be done with software available in high street shops or downloaded from the Internet.
The obvious reason for using steganography as opposed to cryptography is that anything encrypted would immediately draw attention that information is being deliberately concealed, whereas a message sent using steganography, by all appearances, is just another gif image or MP3 file.

Response from Geoff Shively, invisiwall

Steganography is the art of hiding messages inside digital images; or other images in digital images. See http://www.jjtc.com/Steganography/ for some great info on steganography.

Question:

The Cabinet Office in the UK has recently proposed to set up a certification scheme for Information Security professionals (after the debacle with Private Security Industry Bill earlier this year). Is this a good idea and any thoughts on what they are trying to achieve?
(http://www.itsecurity.com/asktecs/sep1201.htm)

Response from Kevin Townsend - ITsecurity.com

There is certainly an argument in favour of some form of certification for security consultants. After all, most serious professions already require this (solicitors, accountants, etc.).
However, given the current UK Government's predilection for regulating everything to do with the Internet, one cannot help but view this move with a degree of cynicism.

There are two parts to this question: is it a good idea; and what are they trying to achieve? Well, WHETHER it is a good idea actually depends upon WHAT they are trying to achieve.

IF the intention is to protect the consumer, then it might be a good idea. On the one hand it might ensure better and more professional advice; but on the other hand it might make users abrogate their own responsibility for their own security. And that would be counterproductive.

However, experience would suggest that this is just another way of trying to control electronic communications. If the desire for control is evidence of paranoia, then this must be the most paranoid government in the history of the UK.

I actually believe that the government discovered this route towards greater control by accident -- but having discovered it, they are unlikely to let it go. So we can expect some form of regulation. Ultimately, there are few serious arguments that we can raise against it - precedents already exist in other professions.

But what we absolutely MUST object to, and defeat, is any attempt by the government to control security consultant certification itself. Any attempt to allow a government body (CESG, for example) to have any say in the certification of independent security consultants will demonstrate that this move is for its own ends and not for the good of the consumer.

We should always remember what my old tutor for studies in British Constitution urged upon his students: "It's not important what we believe they WILL do, it is what they COULD do that is dangerous."

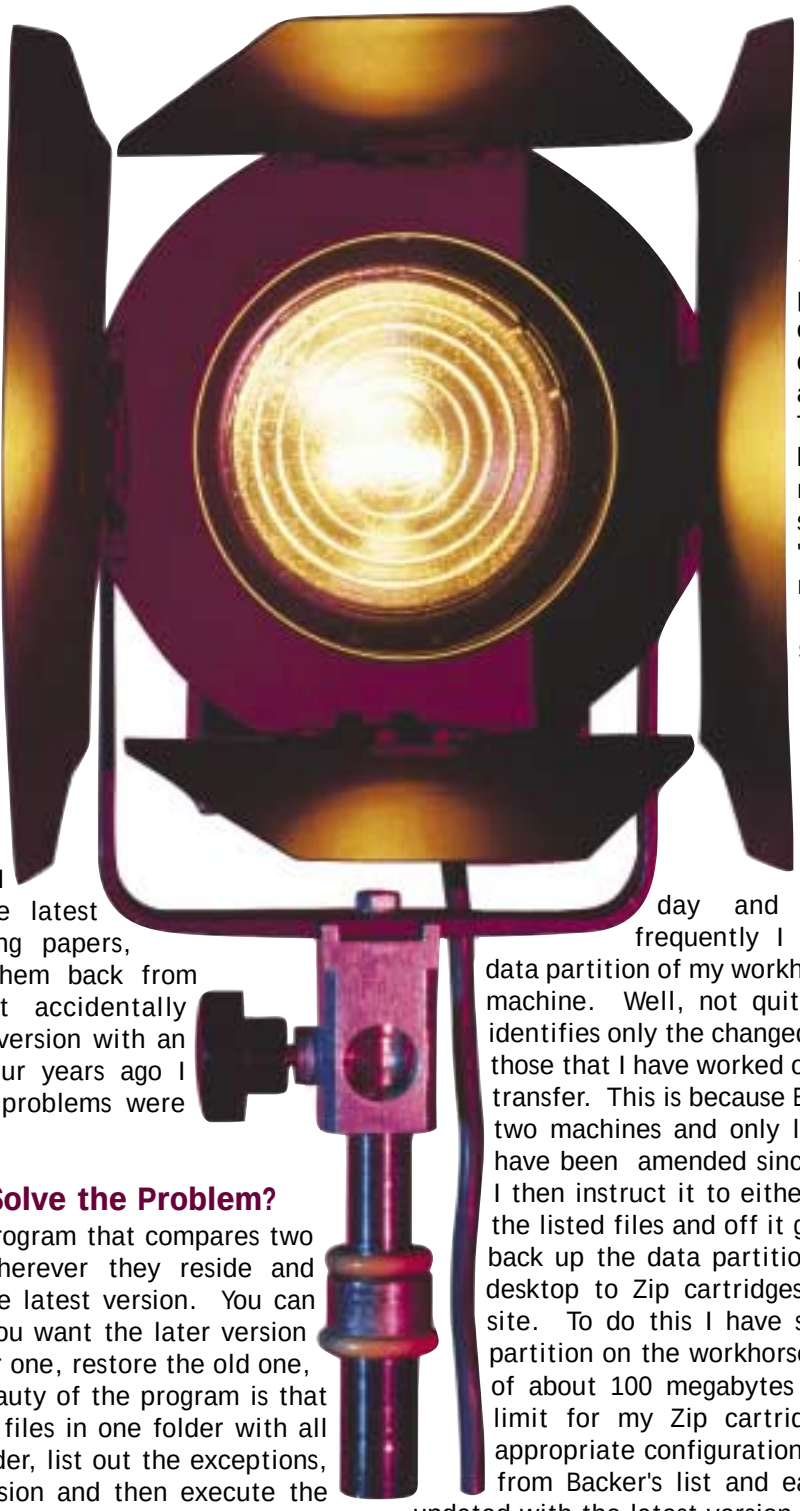
Response from Sarah Carter, HarrierZeuros Ltd

Personally I think the answer is yes, it is a good idea and it is only a matter of time before we are subject to certification. With the quality and value of the advice that our clients ask us to provide, there is no doubt that a time will come when, if the proverbial wheel comes off, they will seek retribution against the individual consultant who provided specific advice that proved to be insufficient or erroneous. There are other industries where individuals have to be chartered or certified before they can provide advice so it does not seem unreasonable to suggest that the same will apply for our industry.

It also gives rise to the idea that we, as an industry will have to provide our employees with liability insurance, rather like directors liability insurance. An interesting idea which will potentially increase the rates we have to charge our clients in order to recoup the additional costs. Once you've involved the insurance industry in this, it will become interesting to see how the certification will be managed. Who will certify and what happens if, for instance, we see a pattern of damages being claimed against consultants who were certified by say John Smith, will liability then get passed onto him and bring in to question his or his (certifying) organisation's credibility as a certifying body? Interesting times.

SOFTWARE SPOTLIGHT "BACKER"

The first of a regular series of articles by JOHN MITCHELL



The Problem

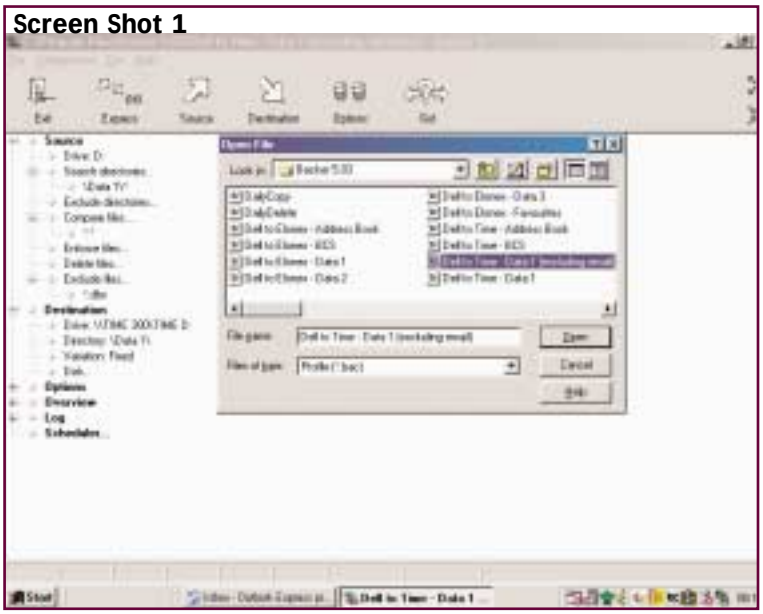
Most people today find a need to back up their work and to transfer files between desk top and laptop on a regular basis. Although Microsoft's Briefcase provides some basic functionality in these areas it is both cumbersome to use and limited in functionality. As someone who is constantly on the move and yet with a need to share information with others I soon found the limitations of Briefcase when dealing with centralised information that was being updated by more than source. I needed to review the latest version of the working papers, annotate them, put them back from where found without accidentally overwriting the latest version with an earlier one. Some four years ago I found Backer and my problems were over.

How Does Backer Solve the Problem?

Backer is a utility program that compares two versions of a file, wherever they reside and decides on which is the latest version. You can then decide whether you want the later version to over right the earlier one, restore the old one, or do nothing. The beauty of the program is that it can compare all the files in one folder with all the files in another folder, list out the exceptions, let you make the decision and then execute the result. It is intuitive, fast and operates within a machine, across different devices on the same machine, or across networks and the internet. Providing you have the necessary privileges you can compare files on different machines across the world.

Take my situation. I have three main machines: my standard desktop, a 'hot start' back-up machine and a laptop. The standard desktop is my daily workhorse. The 'hot start' allows me to get working again very quickly in the event of a failure of my workhorse. Every day and sometimes more frequently I back-up the entire data partition of my workhorse to the hot start machine. Well, not quite. Because Backer identifies only the changed files I only transfer those that I have worked on since the previous transfer. This is because Backer compares the two machines and only lists those files that have been amended since the last compare. I then instruct it to either over-right, or skip the listed files and off it goes. Once a week I back up the data partition on the workhorse desktop to Zip cartridges which I store off-site. To do this I have subdivided the data partition on the workhorse into 20 directories of about 100 megabytes each, which is the limit for my Zip cartridges. I select the appropriate configuration file (Screen shot 1) from Backer's list and each Zip cartridge is updated with the latest version of any changed file.

Screen Shot 1



that I can work on my email away from base and put the whole thing back into synchronisation with my desktop when I get back home.

Give it a try. There is a 30 day trial option.

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

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

Vendor: Leanware (www.leanware.com)

Version: 5.0.3 (as at October 2001)

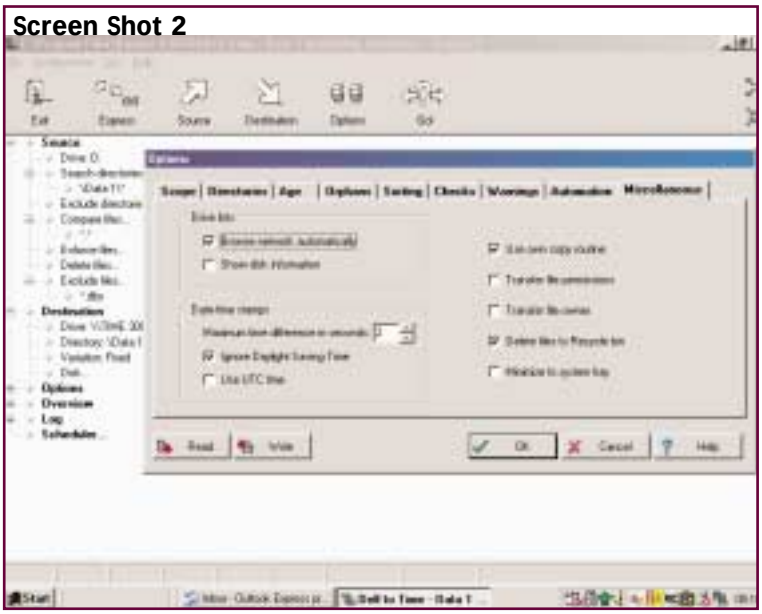
Price: US$ 35 or EUR 35

If I accidentally delete a file from the workhorse I simply load the relevant Zip cartridge, run the compare program and Backer offers me the option of restoring the file from the cartridge.

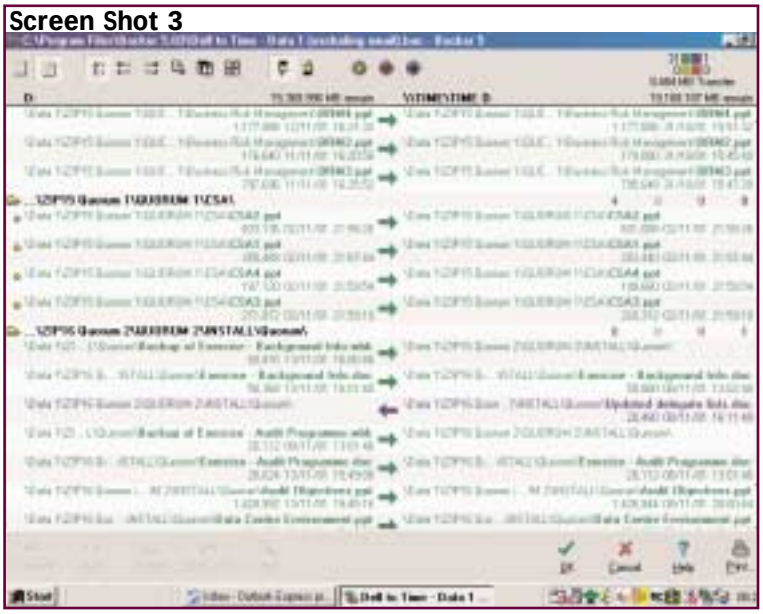
Backer has a nice friendly GUI interface and has stacks of options (Screen shot 2) to let you include and exclude files by name and/or suffix, browse the entire network and do a number of other things that only weirdo's would want to play with.

Because I move around a lot I always do a compare (Screen shot 3) between my laptop's data and that of the workhorse's both before going on the road and at return to base. It only takes a few minutes and eliminates the embarrassment of turning up with that out-of-date presentation! I also update my Outlook Express mail files and address book and my Internet favourites on the laptop so

Screen Shot 2



Screen Shot 3



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

ANNABEL LANE gives an update on the ISACA website.

The Internet Resource List is on page 28

Welcome to another Netwatch column! This one has a slightly different flavour from the norm - I thought we'd take a break from the technical and security sites that are out there for a change and take a look at what ISACA itself has to offer, and what information some of the chapters are making available. We haven't visited the general ISACA website for some time in this column, so it seemed like a good place to start. I was intending to review the web sites of some of the other chapters, including the UK ones. But there was so much information on the ISACA site that I thought merited having its profile raised that I ran out of space. The others will have to wait till next time!

http://www.isaca.org/

So this is the Head Quarters web site. Its home page when I looked was advertising Eurocacs in Budapest, with key links to COBIT, setting out what its purpose is, comments published on it and how you can acquire it, and K Net, which may not be quite as well known. This used to be the GIR - Global Information repository and it aims to provide members with help in identifying and obtaining information on technological change to help us keep pace.

The KNET information is organised into logical categories of interest and concern and it has been identified and peer reviewed to ensure its relevance. You can search on key words and topics or access the categories already listed for you. These range from CISA, IS Security and IS Auditing through to more specific subjects like Ecommerce and telecommunications. If something has a little key beside it that means it is restricted to members and you need an id and password to access it. This information is included in the letter that accompanies your new/renewal membership confirmation and also in the bi-monthly email notice announcing the online availability of each volume of the Journal. Having said that, most of the items seem to be free for all to access. As an example I had a look at the Ebusiness section. Like all the sections, it contains 4 categories of material:

- Education Opportunities
- Books and CD roms
- Articles and papers
- Web resources

I had a look under general resources. There were articles from the Journal (these were the key marked ones) and also papers from people such as Deloitte and Touche, the European Commission, the US government, etc, covering such areas as trusted partnerships in Cyberspace, Cyber crime laws, managing ecommerce security risks, etc.

All in all a pretty good resource to start out using if you are looking for information - and it's a member benefit so we should all be aware of it.

There are of course links to other pages on the home page:

Membership leads to a page on this listing the benefits and with a little program that enables you to identify your nearest chapter. You can request information, learn about ISACA's Code of Ethics, etc.

Chapters, as you might expect, gives a list of all the chapters by geographical area - I was surprised to see how much representation ISACA has in so many different countries. It also links you through to a list of all their websites, should you wish to explore these. You can even see what their seminar programmes are if you feel like attending one. There are a few interesting ones on in India - I wonder how much money my boss has in his budget this year?!

Certification tells you all you could ever possibly have wanted to know about the CISA exam and probably some things you had never thought to ask, or didn't dare to. How to apply, what the domain contents are, how to maintain CISA certification, it's all here. However unless you are feeling particularly brave I don't recommend trying the CISA sample questions. Made me feel as if I had forgotten everything I had learnt.

Publications gives you the option of following a

link through to the book store, where there are reviews and press releases on available publications, links to the journal (if you are a member and information on obtaining books in languages other than English.

Education provides information of professional seminars, training such as CISA review courses and also Chapter events. I didn't know that there was an IS Audit and Control training week - that could be a useful course form someone new to IS audit to attend. You can view the chronological schedule of all the courses and 2002 is already up there.

Research - The Information Systems Audit and Control Foundation (ISACF) actively promotes research that results in the development of products useful to IT governance, control, assurance and security professionals. This page gives you options for how to get involved in supporting their work, what the current projects are and recent and previous deliverables. There is a lot of interesting work being undertaken out there, for example:

- Ecommerce, Controls Audit and Security - in conjunction with Deloitte and Touche
- Virtual Private Networking - New Issues for Network Security (VPN
- Customer Relationship Management (CRM) Project

And that's just naming a few. Unfortunately, you can't get information on the current projects - you have to email the research department for that, but you can access the recent deliverables if they happen to be topics you are interested in.

Standards - a subject dear to all our hearts, of course! This page gives access to the Standards, Guidelines and Procedures for IS Auditing and the Standards for Information Systems Control Professionals. What's the difference I asked myself? There are many more topics under the former, including the Code of Ethics, the standards themselves that you can get in many languages, from Dutch to Japanese and the more detailed Guidelines and Procedures. Hmm, perhaps it's about time I gave myself a little refresher on these! The latter, for control professionals just gives the standards in the 500 number range - Scope, Independence, Competence, that sort of thing. You weren't going to tell me that you had forgotten, were you?

Academic relations - this is an area that I think doesn't get the spotlight on it too much, but this page surprised me. I didn't realise that there were courses and degrees available in IS Controls. They are all of course in the US, but there's still quite a range. You can also download the model curriculum if you want to see what's covered, And of course there's a section on the Academic Relations Committee and how to reach them if you want to get involved.

All the downloads described in the above pages are also available grouped together in one place, which I thought was rather useful - saves you having to flip between pages to access more than one.

There are also quite a few press releases going back several years - I am not sure how many of us still want to read information on experts' opinions on the year 2000 risks, but never mind, it's there if you want it. The most recent one when I looked talked about CISA topping the certification bonus list - that is - the Certified Information Systems Auditor (CISA) designation provided professionals with the highest salary bonus among the 39 technical skills certification programs studied by Foote Partners, according to an article in the August 2001 issue of Information Security magazine. That's quite interesting and reinforces the value of CISA to those who have it. Of course this study was done in the US. But there's a range of things, not just pushing CISA, but also guides and comments released by ISACA.

Should you want to find out what ISACA's vision is and what it aims to do for members, this information can be accessed via the site map. The site map is also the place to visit if you want to put in a request for information or find out who to contact on various subjects at Rolling Meadows. These are very sensibly organised along the same lines as the categories in the eb site review above.

If have any criticisms of the site they would be that it wasn't terribly interesting visually and that there didn't seem to be many links to other useful sites - I am sure this used to be a feature but I couldn't find it. I know that there's a lot of information and that audit isn't exactly the subject that lends itself to snazzy pictures maybe, but there are some sites out there that manage this - like the IIA UK's for example. However, having said that it is very wide ranging and certainly worth book marking.

The new Accord contains significant and onerous requirements for risk management and disclosure. Parties need to mobilise now to achieve compliance by 2005. For example:

- Will your organisation be generating, tracking and reporting operational risk data, including complete and accurate internal loss data, by Basel-specified business line?
- Will your credit risk management and reporting systems contain at least two years of relevant and consistent data.
- Will it be accurately identified and retained to support estimates of an exposure's probability of default and loss given default?
- If your organisation is aiming to adopt the advanced approaches on implementation, will systems have the required 3 years operational risk loss data and 7 years of loss given default data? For these approaches, if robust data collection is not already in place, it may already be too late.

Implications for data

To illustrate some of the issues involved this article considers the high level implications and considerations for credit and operational risk management.

Credit risk management

Just as the three possible approaches to calculate the credit risk element of regulatory capital increase in complexity, so do the data and system requirements.

- The Standardised approach - may be similar to current regulations but the change to using external credit ratings for each counterparty, the increase in collateral types recognised and changes in approach to risk mitigation raises several issues. It will be difficult to source 'solicited' ratings for all counterparties. Providers will have to meet criteria set by the regulator and there will be a greater number of risk weight categories set by the regulator. Some credit ratings will also have taken collateral available into account, in which case further mitigation will not be possible. Therefore, in addition to capturing collateral information, the data will have to be recorded to allow models to recognise when to apply mitigation calculations.
- The Foundation Internal Ratings Based ('IRB') approach - permits organisations to use more sophisticated systems to manage credit risk. Systems should be able to provide data to estimate the probability of default for each borrower and calculate the capital charge based on this, combined with other inputs provided by the regulator.
- The Advanced IRB approach - systems should be able to supply all data inputs to calculate the capital charge.

Potential challenges in relation to adopting the IRB approaches include:

- Realigning internal definitions of default to ensure that the data is consistent with the Basel definition.
- Deciding which exposure specific data should be collected and retained in order to support estimates of the probability of default.
- Deciding on the scale and nature of the investment required to ensure the relevant data is stored in an efficient manner.
- Ensuring consistency with existing data management processes and proposed projects..

The IRB approaches will be a challenge in business areas where data is not typically available, for example new business, areas of very low defaults in a benign economy and other areas such as project finance. Data pooling arrangements could also be a consideration.

Under both IRB approaches, the models will have to be validated regularly to confirm the accuracy and consistency of results on a formal basis that is capable of audit and regulator scrutiny. The requirements for validating the model to the regulator will include retaining data and model details for three years, although this requirement could be waived under transitional arrangements.

The credit risk management approach you adopt will have to be applied consistently through the entire organisation/group. Some operations may not be as advanced as others, so data and systems will have to be harmonised. The extent of diversity in systems between business units, where some will have more advanced models than others, will also increase the risk of delays in system harmonisation.

Operational risk management

There are also three approaches possible to calculate the operational risk element of regulatory risk capital of which the more advanced two, the Standardised Approach and Internal Measurement Approach (or other Advanced Measurement Approaches that may be permitted), have important data and system implications. Organisations will be permitted to allow a mix of these two approaches. Under the Standardised Approach, systems need to be capable of generating

relevant management information and data to calculate the capital charge; ie gross income analysed consistently into the identified business lines.

Flexibility of systems

The Basel Committee has flagged that it expects risk management to be an evolutionary process. Consequently, systems will need to be capable of supporting this evolution in terms of sophistication of models particularly without jeopardising the availability of current or past data for management or disclosure purposes.

Additionally, the Basel requirements are expected to be part of day-to-day risk management processes, so consideration also needs to be given as to how compliant your Customer Relationship Management system will be.

What to do now

2005 may seem a long way away but action is needed now. Whether you wish to opt for a more 'advanced' approach rather than the minimum prescribed, will depend upon how any potential benefits in terms of reduced supervisory capital and enhanced risk management processes is likely to compare with the incremental implementation and operating costs of more advanced systems.

The obvious starting point is to perform a gap analysis of data requirements based upon the Basel standards for the approaches likely to be seriously considered. Key steps involved are:

- Understand what data is available currently and from what systems for each segment of your organisation affected.
- Determine the consistency and cleanliness of your data.
- Understand what you are likely to need for Basel-compliant decision-making and disclosure.
- Compare the present and future data requirements to highlight:
  - New data required and its attributes, such as frequency, granularity etc.
  - What issues of quality, frequency, granularity there are with current data.
  - Which new data will be sourced externally.
  - What scope there is to adapt current systems and technologies to new and reliable risk management processes.

Lastly, you should save money and effort by establishing now which other projects could be impacted by Basel. These will need to be aligned with your Basel project.

Amgad Kamel 020 7311 5686
amgad.kamel@kpmg.co.uk

Growing Basel Data

The risk management systems and related disclosures required by the new Basel Accord have considerable implications for underlying data collection and management.

AMGAD KAMEL provides concise practical advice to those embarking upon meeting these requirements from the data and systems viewpoint.

All you need to know about CISSP

Since becoming a CISSP, **BRIAN SHORTEN** has found, when talking to other security professionals, a great deal of interest in the exam and (ISC)². In this article, Brian answers all the questions he has been asked

What is it?

A CISSP is a Certified Information Systems Security Professional, certified as such by the International Information Systems Security Certifications Consortium, Inc. (ISC)² after taking the exam and fulfilling the certification requirements.

Why take it?

So why did I decide to take the exam and be certified? Several reasons:

- To see if my knowledge was good enough to pass it.
- Because, like CPA for accountants, and CISA for ISauditors, CISSP is becoming an industry standard for Security practitioners which will be recognised throughout Europe and the US.
- To be able to add the pass to my CV.

What does it cover?

(ISC)² has a Common Body of Knowledge [CBK], which is a compilation and distillation of all security information collected internationally of relevance to Information Security [IS] professionals. (ISC)² works to ensure that accomplished and experienced IS professionals with CISSP Certification have a working knowledge of all ten domains of the CBK:

1 Access Control Systems and Methodology
2 Applications and Systems Development Security
3 Business Continuity and Disaster Recovery Planning
4 Cryptography
5 Law, Investigations and Ethics
6 Operations Security
7 Physical Security
8 Security Architecture and Models
9 Security Management Practices
10 Telecommunications and Network Security

What is the exam like?

In format, it is very similar to the CISA exam, with multiple choice questions, and an answer sheet where you fill in the circle, however there are 250 questions, for which you have 6 hours.
I'm advised by (ISC)² that exam papers vary within each exam sitting and change completely over time as the question banks are up-dated. All I can speak of is the exam I took; I found it a tougher exam, because it seems to be more in-depth than CISA.

In particular, the section on law was very US-based (although I understand this is changing to be more International-based), and the technical knowledge required on TCP/IP and OSI levels was heavy. I also had several questions on CCTV, and perimeter fencing and lights!

What is the pass mark?

The (ISC)² website mentions 70% as a rough guideline, but in fact the score required is 700/1000. Different questions (and also different domains) have different weightings. The pass score is set for each new version of the exam. It's based on the questions chosen. SMT manages the whole process to ensure everyone who takes the exam has exactly the same chance as everyone who took the exam before them. (SMT is Schroeder Measurement Technologies, an independent Psychometric testing organisation who manage the whole exam from question setting to re-certification)

How do I study for it?

A CISSP CBK review course has been available in the US for some time. Since the (ISC)² Europe office opened in the UK, the seminar has been condensed for European exam takers. This is a course designed by (ISC)² instructors along with other groups of InfoSec professionals and course documentation writers. This is about to be re-launched - the 2002 version of the CISSP CBK review is 100% new with a full practise paper.

The (ISC)² website has a very long reading list covering all aspects of IS security, from physical security to Unix administration. A useful feature is a link from each book to the relevant page on Amazon.com so you can order the books you need.
Be warned, however, many books are also available from the ISACA bookshop, check and compare prices.
Also, purchasing all books will be very expensive, so think very carefully before filling your basket at Amazon. In fact, I haven't found anyone who bought more than one or two of these books.

Boson.com produce tests for a variety of exams; from Adobe to Sun. I found the CISSP test of 200 or so questions very useful for going over and over the domains - the same strategy was successful for me for CISA.

There is now an official CISSP Prep Guide book, as well as the 'Study Guide' which has always been available for free on the (ISC)² web site . The book is new, and wasn't available when I was studying.
I have good reports though.

What are the Applicant Requirements for taking the CISSP Examination?

CISSP Certification candidates must meet the following requirements prior to taking the CISSP examination.

- Subscribe to the (ISC)² Code of Ethics.
- Have at least 3 years of cumulative work experience in one or more of the ten test domains in information systems [IS] security. Valid experience includes information systems security-related work performed as a practitioner, auditor, consultant, vendor, investigator or instructor, or that which requires IS security knowledge and involves direct application of that knowledge.

No affiliation with any organisation is required for taking the CISSP Certification examination.

Where can I apply to take the exam?

- The (ISC)² website - http://www.isc2.org.
- Talk to Amanda May in the (ISC)2 Europe office Tel: +44 (0)207 779 8215
- See occasional advertisements in Secure Computing Magazine / Information Security Bulletin.

One good thing, there are several exams a year - three in the UK in 2001, with one planned for March 2002. Plans for 2002 publics are to run 10 'public' CISSP CBK Review seminars and CISSP exams throughout Europe. These will include 4 UK exams and reviews. (ISC)² hope to run some additional 'hosted' dates too.

What does it cost (current and approximate)?

- Exam - £309:00 + VAT
- (ISC)² CBK review seminar - £2,040:00 (5 days)
- Handbook - £90:00
- Boson tests - £25:00
- CISSP Prep Guide. - £42:00 (from Amazon)
- CISSP Exam Cram: £25:00 (from Amazon)
- All-in-one: CISSP Certification Exam Guide: £60.00 (from Amazon)

Obviously, only the exam fee is a definite expense, whether the other items are 'must haves' depends on your level of experience and confidence - and the depth of your pockets!

What are the advantages of being a CISSP?

- The personal satisfaction of passing an exam, which demonstrates to those in the know that, you really know your stuff.
- CISSP's are still relatively rare, especially this side of the Atlantic - the numbers are increasing rapidly. In 2001, the number of CISSP's in the U.K rose from 40 to 150. Two of the (ISC)² board members (John Colley and Rolf Moulton) are from the U.K.
- A useful addition to your CV.
- Five!! more letters after your name
- Increased interest from headhunters, I'm told, although I haven't noticed yet.

Re-certification

Like CISA, it is necessary to keep up CPE's, and like CISA you have three years to cover 120 hours. Unlike CISA, however, these hours are split into two headings. Two-thirds (80 CPEs) must be earned in activities directly related to the information systems security profession (Group A). - these are broadly the activities we count for CPE's for CISA. Attending ISACA meetings count; and you can enter your CPE hours on the CISSP pages of the (ISC)² site - very useful. Writing an article published in DataWatch counts for 10 hours.

Up to one-third (40 CPEs) may be earned in other educational activities that enhance the CISSP's overall professional skills, knowledge, and competency (Group B).

Group B Activities augment, enhance, support, and expand the professional's capability, but which are not directly related to information systems security. I.e.

- Organizational Behavior
- Strategic Planning
- Programming Languages
- Programming Techniques
- Tools and Techniques
- Interpersonal Communications Skills
- Interviewing Techniques
- Team Development Skills

If you do not wish to, or you are unable to obtain 120 CPEs, you must retake and pass the exam every three years. In addition, CISSP's must abide by the (ISC)² Code of Ethics and keep their Annual Maintenance Fees up to date (currently $85:00).

My advice would be to make the effort for CPE's - you don't want to take the exam again if you can help it!

Would I recommend CISSP?

Depends on your career path. If you are an IS auditor, join ISACA and become a CISA; if you are a technician, take MCSE, CCNA or similar. If you plan to become a security practitioner, CISSP is the certification you should aim for.

Is it worth the sweat and money?

In my opinion, yes. I passed at first attempt, and only purchased the handbook, so the cost wasn't too high. From the comments and interest from my peers, there is definitely a bonus to being a CISSP, which is one of the reasons I took the exam - and takes us back to the top of this article!

In a previous issue, I wrote about my concerns over 802.11b wireless networking; specifically that they were open to anonymous eavesdropping because they don't have a physical point of contact so it is a good idea for wireless networks should always be considered to be outside a firewall. Some network administrators assume that if 'WEP'(Wireless equivalent privacy) protocol is used they should be secure. Of course, as we all know, it isn't long before any secure system is compromised and so it didn't surprise me to read that a group of researchers from the University of California at Berkeley and Zero-Knowledge Systems have exposed flaws. As the SANS Institute states: "The significance of this discovery cannot be overemphasized: hackers could intercept the transmission of data, read their contents, and modify them without detection." Their site goes onto recommend workarounds - effectively assume it's insecure and build further (but better) layers of defence. There are some ways of configuring the wireless network to make it more secure, for example secure the wireless router / access point (AP), disallow router/ AP administration via wireless, don't send the network ESSID, don't accept the default "ANY" ESSID and of course using a VPN tunnel. But as with most security issues, these things require careful design and periodic review. I am sure that there will be many incorrectly set up systems out there and I hope to be trying out in the near future spy software to judge its real effectiveness.

You may have heard about the generous grant made to the Association by the European Commission, so I thought that I should go international and include some of the news coming out of that often misunderstood body. It is the initiator of much of the UK's legislation and is often the only body capable of acting across country boundaries - so necessary with the internet. An important recent step forward is the so-called 'Convention on Cyber-crime' which was approved by The Council of Europe, an international treaty designed to harmonize laws against crimes committed via the Internet. This treaty will go into effect when five states, at least three of which are members of the Council of Europe, have ratified it. Australia, Canada, New Zealand, Japan and the United States are expected to be among the first signatories to the convention. I cover the effects of this in a future article.

There is also the EC's Action Plan on promoting safer use of the Internet (IAP), one part of a set of policies to deal with illegal and harmful content on the Internet providing support for collaborative projects and other multinational activities covering hotlines for users to report illegal content, improved tools for parental control of children's use of Internet (filtering and rating), and measures to increase awareness of safer use of the Internet. This programme is currently asking for organisations to propose projects to promote awareness of safer use of the Internet - they have 4m Euro to spend at the present time.

Across the pond, Microsoft's Strategic Technology Protection Program (STPP) is causing a lot of heated discussion. This initiative was set up in an effort to help its customers secure their computer systems and maintain that security.

The programme will be implemented in two phases, with the first, Get Secure, launched in October 2001 and the second, Stay Secure, by the end of 2001, according to Microsoft, so it should be out by the time you read this.

The Get Secure phase of the STPP will see Microsoft "working directly with customers to ensure that their networks and computer systems are operating securely". In addition, the company will also offer customers free technical support related to viruses and a Security Tool Kit that includes patches and service packs that address the important security vulnerabilities in Windows NT and 2000, along with the IIS Lockdown tool and documentation. The Tool Kit will apparently include prebuilt configurations for small businesses, end-users and systems administrators. The Security Tool Kit can be downloaded for free and should be available on CD-ROM by the time you read this. All security professions need to be aware of this program - so get a copy now.

The second step of the program will include new security packages made available to customers through the Windows Update website. The service will be free and will offer companies the option to either have the patches automatically applied to their systems, the "Windows Update Auto-update Client" or simply to have them downloaded for later installation.

Some would say this is noble of Microsoft but others would cite that Microsoft software has been at the heart of a number of too many serious security incidents over the past few months. Both the Code Red and Nimda worms exploited vulnerabilities in the IIS web server software to further their spread. Those vulnerabilities had been discovered months before the worms attacked, yet despite this, and despite the existence of patches to correct those flaws, both worms were able to infect hundreds of thousands of computers. This, and the cycle of the patching vulnerabilities, led the research firm Gartner in late September to recommend that companies drop IIS in favour of other web servers until Microsoft took steps to ensure the security of IIS. The inclusion of the Windows Update Auto-update Client for STPP mentioned above is a little suspicious - in order for users to feel safe, they're supposed to sign up for a service that automatically updates their machines with Microsoft security patches!

The Career Column

Adrian Simpson

There are some assumptions, like the world is round and computer auditors are in short supply, which one presumes can be taken for granted.

Therefore, it was something of a rude awakening in the run up to and immediate aftermath of Y2K when the demand for computer auditors fell away. It turned out to be a short aberration and life quickly got back to normal.

I do not know how many people saw it coming, I did not, but the latter half of 2001 again saw the demand for computer auditors and more particularly computer security staff wane. It seems to becoming something of a habit.

Whilst I suppose it would be more stressful if you could not understand why, there are three explanations.

First, Germany, Japan and the US, the three largest economies in the world, are currently all in recession. The UK economy may well escape the worst and it may well all be over in a matter of months, however, many of the multinational groups that employ computer auditors, do not ring fence their UK operations.

Secondly, investment in IT has been curtailed. Many companies in a subdued economic environment, are reducing their investment in new and upgraded IT systems.

Thirdly, the e-commerce boom, whilst not entirely turning into bust, has run a course rather shorter than many expected only a year ago. E-commerce for many companies, rather than fundamentally changing the way they conduct their business, has become just another business channel. The media hype has declined together with IT development budgets. Separate e-commerce initiatives have been moved back into mainstream IT departments.

These three factors, all related, have adversely impacted the computer audit recruitment market. So far, and I do not expect it to go much further, the number of computer auditors who have been made redundant is lower than in a typical year. One of the benefits of depressed capital markets is that it has greatly reduced the number of takeover and mergers. In 2001 they were 70% down on 2000. In any year they are the biggest cause of redundancies.

The only recent significant source of redundancies has been from the big 5 accounting firms. Their recruitment and staffing plans are based not only on attracting new business but also on the basis that a given percentage of those people they recruit as graduates and train, will leave. When they do not, they quickly find themselves overstaffed and redundancies commence.

When fewer vacancies are being generated it does not take long for the supply of available computer auditors to build up. Whilst media coverage of possible recession, terrorism and war tends to incline some to believe it is too risky to move, there is a natural flow of people into the recruitment market. Many, having worked in a company for a given period of time, see no realistic chance of career advancement and others move for purely personal reasons such as the need to relocate. Fewer vacancies means that on average it will take people longer to find a new position and those companies who are recruiting have a larger selection of candidates to choose from.

This translates into a further piece of bad news. When a company is recruiting, if they only have one potential candidate to offer their position to and that person already has another offer, they are more likely to offer a higher salary. If, on the other hand, they have three potential candidates to offer the position to, they may well be less generous with an offer of employment than they might otherwise. Price, which is your salary, is a function of supply and demand.

Whilst such things as contingency planning work as a result of 11th September have helped stimulate demand, the IT industry is currently recovering from an investment boom that nobody thought would stop. The key to an increase in the number of computer audit and security vacancies will be an increase in IT spending to either upgrade existing or develop new systems. This has two effects. Not only does it directly create more work for computer auditors but it creates opportunities for computer auditors to take new positions outside of audit. It is the flow of computer auditors through departments, either to other computer audit departments in other companies or to new positions with their existing employers that generate vacancies. Once that process starts, the number of available computer auditors in the recruitment market will rapidly reduce and the world will once again be round.

Back to Basics

Using CAAT's

In this article, SIMON MOORE goes back to basics regarding the use of Computer Assisted Audit Techniques. He answers the question of why the use of CAAT's is a good idea, outlines the steps that should be followed when using CAAT's (including some of the issues involved) and identifies some of the tricky bits that he has come across in his experience of performing CAAT's. Finally, Simon provides an indication of where CAAT's can be used within the audit of an e-commerce environment.

Why are CAAT's a good idea?

As all of you will be aware the strength of the evidence used to support our audit conclusions is an important consideration when we carry out our assignments. CAAT's allow us, as auditors, to extract and analyse data independent of the systems and personnel involved in the process under review.

CAAT's are ideal when there are large volumes of transactions as we are able to work with the whole population of data. We are able to accurately establish data characteristics and data profiles, which can allow us to target our work on unusual items within the population and so improve our effectiveness.

Given the flexibility of CAAT's and the ability to review all transactions, it is possible that where CAAT's are appropriate, their use will allow work to be performed more efficiently. However, in my experience this efficiency usually translates into an enhanced audit approach rather than time savings in areas where CAAT's have not been previously used.

Steps when using CAAT's

The first task is setting the audit objectives. While these should give the overall direction of the audit tests to be performed it should allow some scope for tests to be established once the characteristics of the population are established.

- **Stage 1: Setting the objectives**

CAAT's are generally used in the substantive testing of transaction or balances, however they can also be used for compliance testing to ensure input controls are operating. Examples of the computer controls that could be tested are edit checks, matching, limit checks, etc.

Audit objectives should be defined before any exploratory work is carried out. Audit objectives should be focused on key audit areas where there are problems in gaining sufficient comfort, as the use of CAAT's is most effective when there is a problem to solve. I would also stress that the audit objectives should be specific and clear.

- **Stage 2: Establish the types of data available**

This will require you to talk to IT personnel, users of the system under review and possibly a review of documentation. It important that you consult with the users as a particular field required for a test may not be populated or may be used in an alternative way. An example of this would be the credit limit field used for debtors. I have found organisations where a value of 1 to 9 is used to describe a status rather than a credit limit, and clearly this would need to be taken in to account when using this field.

- **Stage 3: Obtain file layouts**

This will allow us to determine the fields and files required to complete the audit objectives. Care should be taken to understand flags and codes used within the file. If data is being requested from a third party (even internally), the request for data should be in writing and should include fields, files or reports required, the format of data (e.g. EBCDIC fixed length file), transfer media or method used, request for a file layout to be supplied, date of file, any other special parameters (e.g. only unpaid invoices), time scale for providing files, any security or legal issues as well as reconciliation totals.

- **Stage 4: Obtain data**

One alternative is to obtain the complete file, as this has the advantage of involving less effort on the part of the IT Department as well as preventing a

required field from not being requested. The disadvantage of this approach could be the size of the file, although this is becoming less of an issue as PC hard drives get increasingly larger.

Alternatively, data can be extracted using a query. This has the advantage that only required data is obtained and the format can usually be specified within the query. The disadvantage is that data fields necessary to achieve the audit objectives could be omitted and the IT Department will need to provide assistance in writing, testing and running the query.

The final option is to obtain the data from reports saved to disk. The major advantage of this method is that is possible in all systems. In addition, if reports already exist there will be very little additional work required to provide the data to the auditor. Control values are normally included in the report. Again, the main disadvantage is data necessary for the achievement of audit objectives could be omitted

◆ Stage 5: Performance of the tests and presentation of the results

The first job to be undertaken by the auditor is to reconcile the information to ensure completeness of the data obtained. This is done by obtaining details of the number of records and control values for the records and verifying these to the data received.

Once the completeness of the data has been established the detailed testing can be performed. This should not be performed with blinkers, focussing only on original objectives, it should be inquisitive with you looking for unusual items that may indicate errors. Beware, do not allow yourself to be drawn off on to unnecessary tangents, performing tests because you can, while you investigate unusual items or trends.

Care should be taken when performing the tests as incorrect conclusions could be drawn as a result of errors in processing. With proper planning, issues relating to the use of fields in the wrong way or not obtaining the necessary fields should not occur and the potential for error will be limited to the way the interrogation software is used. Remember to apply the five 'P's!

One function that is susceptible to errors is joining files together. As a result of the one to many relationships that often exist between files the correct identification of the primary file is crucial. To understand what may go wrong you need to understand how the join works. The software selects each record in the primary file in turn and then attempts to match the record, using the selected fields, to a record in the secondary file.

Each record in the primary file is only selected once and is matched against the first occurrence in the secondary file. If you were joining sales ledger master file information to transactions the primary file would be the transaction file with the secondary file being the master file. If the master file were selected as the primary file the result would be a list of customers joined to the first transaction.

The order of steps in a process are performed can have an effect on the time taken to complete an objective. For example, selecting the required items and then joining them to a second file is significantly quicker than joining the complete files and then selecting the items. In some circumstances, the wrong order could also effect the result produced.

Another area where problems can occur is with the creation of formulae. Formulae are used to verify calculations within the application and to aid identification of unusual items. Care needs to be taken when creating formulae as errors can occur through the use of incorrect fields where there are a number of similar fields available or through errors in construction where the formula is particularly complex. The results of formulae, particularly complex formula, should be manually checked on a sample basis to ensure the calculations are correct.

Table 1 lists examples of the types of test that are possible using CAAT's (see page 24)

Using CAAT's in an e-commerce environment

Obviously it is difficult to provide any indication of where CAAT's can be used without setting the environment. For the purpose of this I will consider a company making sales over the Internet with physical delivery of goods.

The first area for review could be to assess the validity of sales. Having obtained the sales transactions we could generate profiles of sales values to gain an understanding of the nature of the transactions and identify items for further investigation. We could summarise sales by customer, summarise sales by date to identify any unusual trends and from an operational viewpoint we could test that all fields required for an order have been populated.

The next area to consider is the completeness of sales. In addition to the analytical review tests described overleaf we could obtain details of goods despatched and match these to invoices to ensure all goods despatched have been invoiced.

Another area for review could be the accuracy of sales. We could test calculations of VAT, calculations of invoice value and ensure the prices charged for goods agree to sales price information. We could also verify the accuracy of key reports used by management.

These tests, plus any others that are required, should give us confidence in the operation of the system and the information being generated from it.

Continued overleaf

Table 1	
Accuracy	
Mechanical Accuracy	Casting the contents of a file
Re-calculation of Fields	Creation of a new field that has been calculated using values in fields and constants.
Analytical	
Stratification	This produces a profile in value bands, dates or codes.
Statistics	This allows a general understanding of the data.
Summarisation on codes	This allows the summarisation of values by selected fields
Ageing	This allows data to be aged.
Validity	
Exception testing	Items of an unusual nature can be identified.
Statistical Sampling	Samples can be selected. The sampling techniques can include random and monetary unit.
Completeness	
Gap testing	Identification of gaps in a sequence.
Cut-off	Using a sequence of reference numbers or dates the cut-off for ledgers can be verified.
Control Testing	
Existence	Testing that fields where input is required contain data.
Duplicate testing	Testing that fields that are required to have unique data not permitted to contain duplicates.
Limit Check	Testing that values in fields that have limits set do not contain values greater than the limits

Conclusion

In summary, CAAT's are a valuable tool that allows an auditor to perform tests that would be difficult or impossible to perform using other techniques. By using CAAT's in a structured way, as described above, you can avoid the pitfalls that can be experienced and take full advantage of their benefit to assist in your audit assignments.

Simon Moore is a Chartered Accountant and Certified Information Systems Auditor. He is a senior manager witin the IS Assurance Department of BDO Stoy Hayward and has spent many years working with CAAT's in a number of environments.

Congratulations to all new CISA exam passers

On behalf of the Board and the membership of the ISACA London Chapter, we wish to congratulate all the CISA exam passers on their success.

Yet again the candidates sitting their CISA examinations at the London centre have shown their outstanding abilities with a 76.7% (77.1 in 2000) pass rate compared to a global pass rate of 50% (52% in 2000).

This year saw another record with 8,210 (6,458 in 2000) candidates registering for the examination globally, and 163 (153 in 2000) sitting the exam in London.

ISACA Members CISA Exam 2001 passes

Mr. Joseph Osei Ackah, IIA
Mr. David Peter Aitkenhead, CA
Mr. Christopher Edward Alston-Baskett
Mr. Kevin Nigel Austin
Mr. William G. Bessell, ACCA
Miss Elizabeth Sarah Bilton, CA
Mr. Stephen Boniface
Mr. John David Browich
Mr. Richard Bunney
Mr. Richard J.B. Jolly
Mr. Andrew Christopher Burton
Mr. Klus Caspar
Miss Anna Cassar
Mr. Glenn Martin Curtis
Mr. Deepak Damania, ACA
Mr. Adrian Robert Davison, CISSP
Miss Michelle Li-Ming Foong
Mr. James Gallen
Mrs. Sharon Ruth Gebhard
Mrs. Ann George
Mr. Nicholas John Gtinatsis
Mr. James Gordon
Mrs. Carol Anne Gradwell, PIIA
Mr. Peter Mark Harris
Mr. Ian P. Hay, HNC
Miss Jennifer Sarah Houston
Mr. Sayed Shahab Hussein
Mr. Roger Per Ivar Isaksson
Mr. Martin Jaros
Mr. Diogu Sunday Kalu, CA
Mr. Gopal Kharbanda, QILA,FLC
Mr. Jurg Kisseleff
Ms. Christine Ann Lewis, MIIA
Mr. Daniel Longhurst, CIA
Mr. Angus Maclean
Mr. Daniel McDonough
Mr. Nick James McLelland
Mr. Paul C. Merison
Mr. Lachezar Metodiev
Ms. Mandy Miller
Mrs. Susan Sheila Milton
Mr. Ivor Anil Misquith, CA
Mr. Massimo Noro
Mr. Charles Roderick Offer
Miss Yen Leng Ong
Miss Natasha Peyto, ACCA
Mr. Martin Plummer
Mr. Paul Bertram Reed, ACA
Mr. David William Roberts, AGA
Mr. Adin Robinson
Mr. Andrew James William Robinson
Mr. John E. Roder, ACCA
Mr. Martin Peter Savill
Mr. Purshottam Nandlal Sharma, CA
Mr. Max Adam Sherwin, ACCA
Mr. David James Simcox
Mr. Kalwinder Kumar Taheem, PIIA
Mr. Benjamin Stirling Taylor, CA
Mr. Mark Turley, CPFA
Mr. Helgaard Delarey van Rooyen, CIA
Mr. Sriram Venugopalan, CA
Mr. Steven Williams
Mr. Robert W. Wright
Mr. Sutton Tat-Sang Yeung, CIPFA

Non members CISA Exam 2001 passes - awarded CEP membership

Mrs. Beatrice Akintomide, ACCA
Mrs. Dana R. Albu
Mr. Michael Ball
Mr. John Frederick Bazley
Dr. Mark Bleackley
Mr. Scott Michael Bolderson
Mr. Edwin Norman Bowden
Ms. Barbara Karen Burden
Ms Shirley Anne Cardus, PIIA
Mr. Graeme Richard Carruthers
Miss Joanne Cash, CIA,CA
Mr. Jean-Yves Anthony Clarke,
Miss Amelia Anna Cocca
Mr. William Roger Coffey
Mr. Ben John Cooke
Mr. Jonathan C. Day, ICAEW
Mr. Stephen William Dellow
Mr. Timothy R. Depledge, ACA
Mr. David J. Edwards
Miss Stephanie Eyre
Mr. Jeremy Garland
Miss. Julie Gillhespey
Mr. Keith Goddard
Mr. John Hall
Mr. Jonathan James Holden
Mr. Julian Michael Hunt, ACA
Mr. Jagmeet Singh Kang
Mr. Dinesh Karunadhara
Mr. Viacheslav Katok, CA
Mr. Paul D. Kelt
Mr. Robert T. Kidd, ACA
Miss Jacquetta Mary Lavinia Lee
Mr. Stephen Licence, MIIA
Mr. Graham J. Little, CA
Mr. Bertrand Livinec
Mr. Andrew Lopokoiyit, MCP,MSc
Mr. Ryan Loughins
Mr. Stuart Campbell McArthur
Mr. Dominic Richard Mooney
Mr. John David Nunn, BSc,ACMA
Mr. Stephen Robert Pilditch
Mr. Simon T. Pilkington
Mr. Christopher Francis Poole
Mr. A. Gilles F.L. Pun-Lai-Yue
Mr. Christopher Reed
Sr. Alejandro Ripol
Miss Anna Shah, ACCA
Mr. Kian Shroff
Mr. Andy Skelton
Mr. Laurence Slavin
Mr. Timothy Simon Smith
Mr. Steven Snaith, CIPFA
Mr. Simon Still, CA
Mr. Andrew William Strong, CA
Mr. Christophe Sutehall
Mr. Craig Taylor, ACIB
Mr. Kevin Tilbey
Miss Sarah E. Walker
Mr. Peter Donald Wilson,
Mr. Michael Wilson, PIIA
Mr. Alan J. Wright
Mr. Sajid Yacoob

Special congratulations to the following ISACA London Chapter members who achieved top scores in this year's examination:

Mr. Roger Per Ivar Isaksson
Mr. William G. Bessell, ACCA
Mr. Daniel McDonough
Mr. Christopher Francis Poole

Please note: this list excludes individuals who requested their exam results NOT be released

INSTANT MESSAGING

Great business tool but what about security?

Allan Boardman CA(SA) CISA CISSP

Instant messaging (IM) has for some time been very popular with non-business users for keeping contact with friends and family and is now starting to take a hold in the corporate environment. It provides an inexpensive, quick and easy way to communicate, the software is generally free, and as an alternative to mail or email, it is considered to be more immediate.

It is viewed as an important technology for companies wanting to improve collaboration efforts and communications between staff and business partners. Vendors are quick to point out that IM is the next great business tool and there have been some predictions that IM will surpass email as a corporate communications tools in the not too distant future. The recent and phenomenal growth in text messaging (a related technology) may well spill over into the corporate IM space.

All this points to employees embracing IM technology with a passion and often without management's knowledge or approval, thereby leaving the growing risks unchecked. In the absence of IM provided by their employers, workers are signing up to free services offered by AOL, Yahoo and MSN. As a result, company networks are being unwittingly plugged into third-party systems that aren't secure, reliable or adequately policed. This potentially provides an easier entry point for hackers and virus writers concentrating on other channels into the corporate network as email gateways and firewalls are becoming increasingly locked down. The uncontrolled use if IM at work can potentially open the door to viruses, denial of service attacks and identity theft. In addition, in most cases, sensitive information exchanged via these networks cannot be tracked, logged, saved or audited.

Instant messaging is still a relatively immature product from a management and control perspective. Corporates therefore have to choose between implementing dedicated IM software now, or waiting until it becomes a more integrated feature within broader enterprise communications products.

Risks associated with using IM include:

- Password security - logon credentials are not encrypted or protected when transmitted across the internet. Users should therefore ensure that they do not use the same credentials as for the other corporate systems.
- Viruses and trojans - enables viruses to enter networks via attachments and provides an easy entry point for the installation of trojans, giving the hacker almost total control of that computer.
- DOS attacks - vulnerabilities have been identified whereby users could send a string of characters and crash the other persons messenger program and/or the machine itself.
- Confidentiality and privacy - in most cases, messages and file transfers are not encrypted, and can therefore be subject to snooping or tampering. Most of the existing IM providers specifically advise against sending any sensitive material using IM.
- Authentication - generally weak, which enables hackers to take over IM accounts and impersonate their owners.
- Software vendor access - messages flow through and are stored on the vendor's systems, generally in an unencrypted format.
- File transfers - infected files can bypass normal corporate virus scanning and monitoring systems.
- System management features - as the products have grown from being consumer based

products, they are generally user friendly but lack basic system management features.

- Quality of service - organisations have to rely on externally provided services, generally built for non-business use.

- Support - as the products are generally free, limited support is provided by the vendors.

- Interoperability - Not all IM systems will work together, and there is a general lack of standards, even between the major players such as AOL, Yahoo and Microsoft. While this non-interoperability persists, workers who want to IM all their friends, partners and customers may find it hard to resist installing rogue IM applications behind management's back.
- Auditing of conversations - the absence of logging means that monitoring of client communications is restricted, which may have compliance ramifications.
- Legal - contracts with business partners may have to be revised to take account of this form of communication.

Security vendors are starting to take notice and have made some efforts to provide security plug-ins to create IM systems more suited to business. Command Code, for example, offers a PGP encryption plug-in for MSN messenger, and Jabber offers a platform aimed at enterprises, among others. FaceTime Communications has released a product called IM Auditor which they claim can plug in to all the different IM networks to enable more effective management of IM communications.

Instant Messaging is clearly here to stay and may well turn out to be as great a business tool as email and the browser. If you don't like the sound of IM in the office, it may be too late to stop it. Overly strict rules and clamping down IM's rollout to the corporate desktop may exacerbate the problem, as has proven with overly strict email and internet usage polices which has resulted in more dangerous unauthorised use in the past. A reasonable usage policy might be the only option, combined with measures to secure and monitor the IM traffic entering and leaving the network.

Allan Boardman, CA(SA), CISA, CISSP, works in information security at an investment bank in London.

allan@internetworking4u.co.uk

There are dates for birthdays, holidays, changing tides and the CISA exam. If you have an interest in anyone of those dates then you will probably plan for them, and once they are in your favourite diary or organiser then you'll probably never forget them. Out of this group my favourite date is Saturday June 8th 2002, that's the day of the next CISA exam. Why, there is no need to worry about it - it's just so far off. At the time of writing, my personal commitments are several family birthdays, school holidays, the busy work period till Xmas, then the Xmas break; another busy couple of months. Once the days lengthen there's more daylight time in the evening for outdoor sports, hobbies, yet more school holidays and the Easter break. By now its late April early May and the CISA exam is the first Saturday in June. Not much time left to revise. I wonder what the exam questions will be like? Panic!

Planning to Pass

Fortunately, I am now receiving a steady stream of enquires from prospective candidates. This indicates that the majority of individuals are well aware of how time slips away and are now preparing their individual revision plans to ensure success on examination day.

The CISA professional certification program, which includes the examination, goes back to 1978. Its aims are to assess your level of proficiency in performing computer audit or computer security related work. It presupposes that you already have knowledge of the subject material by virtue of your experience.

ISACA, at international and national levels, provide an extensive range of materials and learning opportunities to help candidates pass the exam. There are no structured study modules although ISACA annually produces the `CISA Review Manual', which briefly covers all the domains and provides practice questions. Learning the contents of the manual will not, in itself, provide sufficient knowledge to pass the examination. The International office also publishes a 'Candidates Guide to the CISA examination' which includes a recommended reading list. The London chapter of ISACA annually runs a CISA Review Course. The aim of this course is to help candidates prepare by ensuring that they are familiar with the nature and structure of the examination and have sufficient practice in answering examination style questions.

Useful resources and suggestions:

The following suggested resources will help you plan for your examination success. They are also fun!

- The ISACA International Web-site resource at www.isaca.org contains all the current information regarding the examination process and revision aids. Favourite links within the site are bookstore, certification and KNET.
- London Chapter Members meetings provide an opportunity to share experiences with fellow colleagues, and have a drink. The programme of events is available at www.isaca-london.org
- Ensure you have current copies of the CISA review manual and the CD containing sample questions and answers. They are both available form the ISACA bookstore at www.isaca.org.
- The London Chapter run computer audit training days and a CISA review course. Details are posted on the London Chapter Website at www.isaca-london.org and via the Chapter Newsletter, as they become available.

Michael Christodoulides, CISA

INTERNET RESOURCE LIST

AUDIT

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

SECURITY

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

COMPUTER COMPANIES AND SYSTEMS

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

OTHER ORGANISATIONS

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

HACKERS AND VIRUSES

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

AREAS OF AUDIT INTEREST

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

Answers to Word Puzzle on page 3.

The "unchecked" letters spell the word SECURITY