IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

JOURNAL

volume 12 number 3 spring 2002 ISSN 0961-9348

Programme for members' meetings 2001/2002 season

Tuesday 2nd October	**Windows 2000 Security** *Configuring NT securely is often a major hurdle - Windows 2000 adds many new challenges to a secure infrastructure. Risk minimisation strategies include: reviewing typical threats; using W2K security mechanisms pro-actively; customising administrative control; planning and implementing counter-measures securing Active Directory; the encrypting file system.*	Evening 16.00 for 16.30 to 18.00 KPMG
Monday 12th November	**Outsourcing & Out of Control Projects** *About 25% of software projects will be cancelled because they are late, over budget, have unacceptably low quality, or experience some combination of these problems. Outsourced operations have created new security threats and risks. Practical control measures are vital. The risks associated with outsourcing overseas and ecommerce operations will be considered.*	All Day 10.00 to 16.00 ICAEW
Tuesday 4th December	**Network Security & Management** *Changes in the technologies underlying computer networks are important to auditors because these have implications both for network security management and the audit of these arrangements. These implications provide today's theme concentrating by way of example on the audit of ATM (Asynchronous Transfer Mode) and Frame Relay.*	Evening 16.00 for 16.30 to 18.00 KPMG
Tuesday 29th January	**Internet Security** *The theme of the day will be internet security, but particularly Intrusion Detection systems. These are automated systems that monitor communications and operating systems, alerting operators of potential hacking attacks.*	All Day 10.00 to 16.00 Royal Aeronautical Society
Tuesday 12th February	**The Subversive Spreadsheet** *"A spreadsheet application can subvert all the controls in all other parts of an information system" (R. Butler, VAT Auditor, Customs & Excise). This talk by presenters from The European Spreadsheet Risks Interest Group shows the evidence. It discusses the risks, the audit and preventative methods*	Evening 16.00 for 16.30 to 18.00 KPMG
Tuesday 5th March	**The System's Down - Again!** *The unavailability of computer systems can give rise to serious problems for the continuing operation of the business. The ability to deal with or prepare for these problems is critical for business survival. The theme of the day is how business minimises their risk and will include high availability options, problem management and business continuity.*	All Day 10.00 to 16.00 Royal Aeronautical Society
Tuesday 14th May	**Data & The Law** *The legal risks and issues associated with IT and networking are not always well understood and often underestimated. This update on a fast changing area of the law is aimed at meeting the needs of risk management/audit professionals and providing opportunities for debate and discussion.* **This will be preceded by the Annual General Meeting.**	Evening 16.00 for 16.30 to 18.00 KPMG

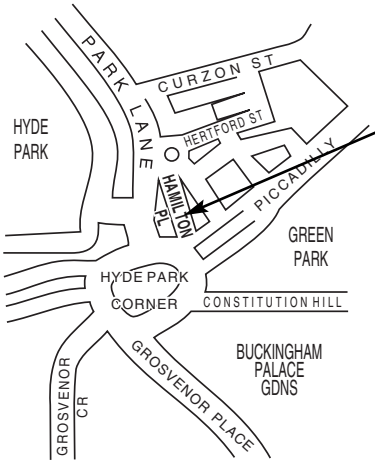
The late afternoon meetings are free of charge to members.
For full day briefings a modest, very competitive charge is made to cover both lunch and a full printed delegate's pack.
For venue maps see inside front cover.

visit our website at www.bcs-irma.org

Contents of the Journal

Venue for

Full Day Technical Briefings

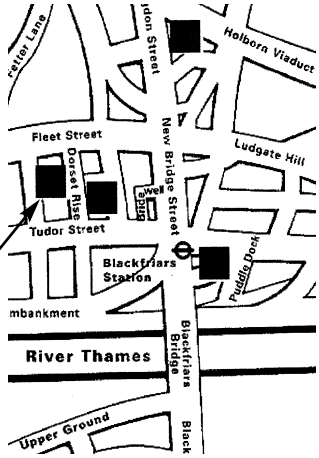


Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ

KPMG
8 Salisbury Square
London EC4

Venue for

Late Afternoon Meetings



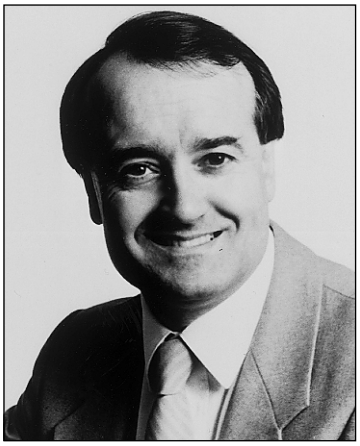
The ***Journal*** is the official publication of the Information Risk Management & Audit Specialist Group of the British Computer Society. It is published quarterly and is free to members.

Letters to the editor are welcome as are any other contributions. Please contact the appropriate person on the editorial panel.

Editorial address:
47 Grangewood,
Potters Bar
Herts, EN6 1SL
Email: john@lhscontrol.com

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by PostScript, Tring, Herts.

Editorial



I am often asked to review business continuity plans and over the years have noticed a regular problem with all of them. Every one that I have looked at has assumed that only their firm will be facing a disaster at a particular moment in time. There seems to be no concept of what I call a community wide disaster, where many firms are hit simultaneously, along with the associated infrastructure such as transport, power and telecommunications. The defences that are often offered falls into two categories: first, it is too complicated to cater for every scenario and second everyone else will be in the same boat anyway, so why worry? I have some sympathy with both views and I have usually found that management are usually very good at crisis management when unforeseen problems occur. On the other hand I do know of a number of people whose health has been significantly impaired when attempting to recover from a disaster without a suitable plan being available. The other problem that I notice is the assumption that all the key staff will be available for recovery purposes. This is so unlikely as to be preposterous and I have often 'umpired' recovery tests when as soon as I say that certain people are not available the whole thing falls apart. Where is this all leading? Well, we have two articles in this edition that deal with business continuity. The first by Alphus Hinds looks at the potential problems faced by Indian Railways if their computer systems are compromised, while the second by Andrew Cormack examines security in universities and colleges. Having worked in both the transport and the university sectors I can appreciate the problems faced by both.

Rupert Kendrick, our new events reporter provides an insight into our latest two events. The first a full day briefing on internet security and the second on the subject of the 'subversive spreadsheet'. Both sessions were extremely well attended and perhaps Rupert's write up will encourage you to come along to our events.

Andrew Hawker examines a cure for the ISISTS syndrome in his regular web column and Colin Thompson does his usual sterling job in keeping us up to date on matters of our parent body. Colin mentions the new code of ethics, which I intend to publish in the next edition of this Journal.

Bob Ashton, our Australian Correspondent, reports on action taken by the Australian government to bring their data protection legislation in line with that of the EU. Bob has also pointed out to me the unusual symmetry of a date/time combination on the 20 February 2002. At 20.02 on that date we had the situation where a 24 clock calendar would have read 20.02.20.02.2002. But only for those using the European date format Bob. Our American cousins will have to look elsewhere for their symmetry. According to my calculations the next symmetric European date will be 20:03 on 20 March 2003.

A reminder that our AGM is scheduled for the 14 May. This is your opportunity to grill your Committee on its stewardship of your specialist group. You will also find a nomination form for applying to join the Committee. I seriously encourage you to do so.

There were no takers for the prize of identifying the key phrases in the '231 Rules of Survival for Evil Overlords, or Heads of Audit' column in the last edition, so I guess I will just have to swig another bottle of bubbly in celebration of defeating you all once again!

Finally, back editions of the Journal can be found on our web site, along with a host of other useful information and links. I urge you to point your browser to **www.bcs-irma.org.**

Happy reading and I look forward to seeing many of you at our meetings.

John Mitchell

Down Under Report

Bob Ashton – Australian Correspondent

Recent Legislative Developments

The Commonwealth Privacy Act 1988 was amended from 21 December 2001 to include 11 National Privacy Principles. These are:

1: Manner and purpose of collection of personal information;

2: Solicitation of personal information from individual concerned;

3: Solicitation of personal information generally;

4: Storage and security of personal information;

5: Information relating to records kept by record-keeper;

6: Access to records containing personal information;

7: Alteration of records containing personal information;

8: Record-keeper to check accuracy, etc., of personal information before use;

9: Personal information to be used only for relevant purposes;

10: Limits on use of personal information;

11: Limits on disclosure of personal information.

This has prevented the possibility of disruptions to Australia's trading relationships with the EC.

These principles have also been incorporated into the Queensland Government Information Standard 42, which has recently been made mandatory for Government Agencies.

The Queensland Government has also recently issued its Information Standard 18. This is based on the principles contained in ISO/IEC 17799 Information Security Management, formerly known as Australian Standard AS/NZS 4444 in this part of the world. Currently, Queensland is the only state in Australia to have adopted this internationally recognized level of security for its own infrastructure.

Supporting the Standard are the IS 18 Information Security Best Practice Supplement and the Information Risk Management Better Practice Guide. I have found the latter guide to be very useful. The processes outlined in the guide were developed in line with the current *Australian Standard for Risk Management AS/NZS 4360:1999, HB 143:1999 Guidelines for managing risk in the Australian and New Zealand public sector* and the MAB-MIAC Advisory Board – *Guidelines for Managing Risk in the Australian Public Service (1996)*.

The purpose of the guide is to explain the principles which should be followed in adopting risk management in Information Systems, and is very successful in this.

These document are freely available from:
diiesrq.qld.gov.au, under publications.

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should either be on double spaced, single-sided A4 paper, e-mail, or in Microsoft Word, Word-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality monochrome photograph, or electronic image.

Submission Deadlines

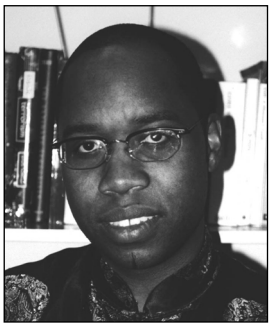
Spring Edition	7th February
Summer Edition	7th May
Autumn Edition	7th August
Winter Edition	7th November

"The New Risk Paradigm"

for Indian Railways as Part Of India's Tomorrow

(A Discussion Paper)

Alphus Hinds



Introduction

Prime Minister Shri Atal Behari Vajpayeeji, has heralded India's arrival into the Information-Age, by defining Information Technology (IT) as "India's Tomorrow". This mantra has been embraced by the nation at large and by Indian Railways embarking upon a radical modernisation program.

Indian Railways will have a dual role to play; one as an accomplished IT exploiter and the other as a facilitator of the Information-Age on the Indian sub continent. This will be in keeping with the long held notion of Indian Railways, as the nation's lifeline.

"Since their inception, Indian Railways have successfully played the role of prime mover to the economy and society of the Indian sub-continent. In the process, Indian Railways have become a symbol of national integration and a strategic instrument for enhancing our defence preparedness[1]."

In preparing for India's Tomorrow, Indian Railways must protect the rail network by preparing for the Threats of Tomorrow Today (3T's). Failure to do so will compromise public safety, economic and national security. This fact was alluded to in the Railway Budget 2000-01 when it stated Indian Railways "have a strategic value next only to the armed forces.[2]"

As already acknowledged, full modernisation means an aggressive adoption and reliance on IT, which in turn will expose Indian Railways to the 3T's; the magnified threats, vulnerabilities and risks of today with those of tomorrow. The Railways, now a part of India's growing interconnected Critical National Infrastructure, is placed squarely in the firing line. Now an interest to the plethora of adversaries, such as the hacker, the cyber-terrorist and state sponsored Information Warfare attacker.

The Indian government through the corporate rail executive must publicly demonstrate their credentials as to being adept at preserving public safety and IT security in the cyber environment. An environment which will increasingly underpin the integrity of the physical rail infrastructure and operations. Failure to do so will be a dereliction of their mandatory duty of care to the citizen and to the rail customer.

The challenge has been defined…what will be the response?

This paper draws on international experience when asking questions from the emerging 'thinking'. All in an effort to maintain the primary mission statement[3] of any modern high-density rail network, as it becomes part of a nation's internet-based Critical National Infrastructure.

A Retrospective On Rail Modernisation

The impetus behind modernising railways, particularly towards the later part of the 20th century, has revolved around safety, high-density traffic flows, infrastructure reliability, reducing operational costs and harnessing income from non-traditional sources. These competing forces have not made for a smooth linear progression of advancement. Rather, a picture of stilted development emerges. A picture, which reflects the different strata of prevailing political climates, "knee jerk" media driven sensationalism and economic expediency.

So, what type of modern railway legacy is this giving rise to? May I suggest, a modern high-density rail network, stripped of its traditional layers of mechanical and operational redundancy. Instead, these are replaced by a web of discrete mission critical environments. Such environments have created a railway network more vulnerable to single points of failure. Great advances have been made in safety, reliability and in efficiency, but to what extent are we sowing the hidden seeds for the electronic (cyber) and asymmetric physical attack? These attacks are going to occur and have the potential to exact a heavy toll on the safety of customers and staff, train services, rail infrastructures and financial revenues.

Too often, the modernising railway has failed to truly comprehend the comparable leap required in organisation and management philosophy to cope with IT dependency and prepare for the electronic (cyber) and asymmetric physical attacker.

The transition from kinetic to a cyber dependency is ushering in a change in the *modus operandi*; a subtle one, but a change nevertheless. A response is required, such as understanding the dynamics of Risk Displacement from front line operator to embedded software technology e.g. from train driver to Automatic Train Protection system and on board command and control communication systems.

The growing cyber dependency presents uncertain consequences for security and safety. Railways must become better equipped to manage and plan for cyber driven uncertainty. By adopting techniques such as "Gaming[4]", this will assist in minimising the risk of security and safety becoming a casualty of modernisation.

Will the modernisation of Indian Railways create an apparent contradiction of terms – a safer but less secure railway? This is a rhetorical question, which must be asked throughout the modernisation process, as a pause for thought; remembering, security is the 'flip-side' of safety.

---

1 Status Paper, on Indian Railways, Government of India Ministry of Railways (Railway Board) 27th May, 1998

2 Speech of Kumari Mamata Banerjee, Introducing the Railway Budget, 2000-01 on 25th February 2000

3 to reliably move the maximum number of people and goods within a secure and safe environment over their chosen journey.

4 Strategic Scenerio role play (eg. War Games)

Threat Uncovered

Considerable experience in dealing with the Kinetic threat and risk has been gained by railways from around the world. Now, railways must build upon this experience to address the electronic threats aimed at their information asset base. For many, nothing less than a cultural mind shift will be required.

Indian Railways have recently experienced violent acts of terrorism with the bombing of stations and other sensitive installations; bridges, track, trains etc. How will this type of terrorism evolve in a post modern IT dependent Indian Railways? How long before the IT or information assets becomes the target? Indeed, has a cyber front already been opened?

A case in point is the proposed Indian Railways utilisation of their own Right of Way (ROW) "for building a nation-wide broadband telecom and multimedia network by laying optic fibre cable (OFC)[5]." Will this prove an irresistible target for the terrorist? One attack could have a ripple effect into mass disruption; not only disrupting the Indian Railways' own telecom infrastructure but also that of telecom operators and Internet Service Providers (ISPs). What protection will be required? How vulnerable will SCADA (Supervisory, Control and Data Acquisition) systems be in the Indian Railways to electronic (cyber) attack? Does Indian Railways have a management mechanism to decide:

- When IT systems are under attack?
- What should be the real-time response?
- What level of risk this represents?
- How best to preserve electronic evidence so it is admissible in a court of law within and outside of India?

Could this all sound a little too melodramatic or even implausible? If one begins to examine, let's say, the anatomy of terrorism in Asia, evidence could suggest a growing interest in all things cyber; with a likely evolutionary trail with the following notable hallmarks:

1. **Computer assisted attack:** planning, co-ordination, data exploitation using computers, Internet.
2. **Computer enhanced attack:** exaggerating consequence of attack e.g. explodes a bomb at a railway station and disrupts the '000' Emergency Services System by Caller I spoofing[6] for a denial of service
3. **Full Cyber attack:** computer systems and information assets are the sole objects of the attack to cause the desired physical effect i.e. loss of life, mass disruption etc.

Terrorist activity in Asia, as in India, tends to be fundamentalist or state sponsored with close links to organised drug crime. With the resources of a state or drug cartel to draw upon, the terrorist groups will acquire the expertise.

Railways have already had salvoes fired across their bows. As in NYC, hackers hacked the electronic signs in a Manhattan subway changing the message display. Hackers raided Chinese railway computers in a six-month ticket fraud scheme, that began in June 1998. Benign, or the beginning of something more sinister?

Preparing for Threats of Tomorrow Today (3T's); the magnified threats, vulnerabilities and risks of today with those of tomorrow, must become a recurring theme within the modernisation of Indian Railways. It is good to remember that threats exploit vulnerabilities, not create them.

Table 1 represents a growing consensus of opinion, which a responsible rail environment cannot ignore.

Defining The "New Risk Paradigm" for Indian Railways

How can we define "The New Risk Paradigm"? It is the risk we run of failing to articulate through Policy to Strategy to Operation, the protective measures required to secure information assets or IT dependency from:

The Nuisance Hacker –
Thrill seekers not looking to do serious damage
……The Hacker!

The Focused individual or group –
Seeking benefit or wanting to do damage
…… The Attacker!

The National effort –
Well financed, intelligence supported, strategically focused
……The Information Warrior!

The protective measures must be considered as part of the wider picture of a nations' Critical National Infrastructure. **"The New Risk Paradigm"** is only 'New' if it is not given the credence it deserves.

Indian Railways, as with other modernising and advanced railway networks, must 'DBOM'….

D evelop
B uild-In
O perate
M aintain

…..cost effective protective measures for their growing IT dependency. Finally, we are left with one question for Indian Railways:

As the nation's lifeline, will the modernisation process of the Indian Railways be in the 'vanguard' in helping to build the defences for India's tomorrow?

ADDENDUM: A Special Consideration - Calcutta Metro System

Rapid Mass Transit Commuter Rail Systems (The Metro) have become the indispensable backbone of the commuter transport task for most major cities. Often these systems are congested and are under immense pressure from the volume of demand and, particularly in Europe, ageing infrastructure.

History bears testimony to extreme acts of violence against Metro systems, which still represent relatively 'soft' targets for extreme groups to exact multiple casualties and cause major disruption. What has changed is the potential method of attack with the use of Chemical, Biological and Radiological (CBR) agents as well as cyber and information warfare techniques.

5 Speech of Kumari Mamata Banerjee, Introducing the Railway Budget, 2000-01 on 25th February 2000

6 Spoofing attack is like a con game to deceive a victim into making an inappropriate security relevant decision

Table 1: Sources, Type and Nature of Security Threats

Source of Security Threat	Type of Threat	Manifested Nature of Threat
Insiders	Disgruntled employee Ex-employee Paid informant Compromised or Coerced employee	Corruption, destruction, exploitation of information asset (eg. Virus, logic bombs, worms) Tampering/removal of vital equipment Facilitate access by third party
Hackers	Institutional Hackers Recreational Hackers	Denial of service attacks Malicious code e.g. Virus, worms Theft & exploitation of data
Industrial Espionage	Economic competitors Official intelligence organisations	Theft of business intelligence Theft of proprietary information
Nation States	Other countries (adversaries)	InfoWar Techniques Computer network attack Computer network exploitation HERF, EMP devices
Terrorism and Terror Crime		Target data/hardware Data Attack compromises of - Integrity: Insertion,deletion - Confidentiality: Exploitation - Availability: Denial of Service Hardware Attack (remove, destroy) e.g. HERF, EMP devices

Key: HERF = High Energy Radiation Frequency. EMP = Electro Magnetic Pulse

The hypothetical became the reality on March 20, 1995 with the Sarin gas attack on the Tokyo subway system by the Aum Shinrikyo cult, killing 12 persons and impairing the health of 5,498.

Since this attack, major metropolitan Metro Rail Systems have had to address the CBR threat in earnest. What upgrades would be required in their dynamic protective systems in order to secure the metro environment and discharge a responsible public safety strategy?

Key questions such as:

- Should an early warning system of sensors be installed to detect CBR agents?
- Where should such sensors be installed on a Metro network?
- At what threshold of detection will an evacuation or closure be initiated?
- If agents are detected, what should be the response; vent to outside or contain?

These questions have been asked with varying responses and ensuing actions by Metro Rail Systems such as the Washington DC Metro, London Underground, State Rail Authority in NSW, Australia.

The Calcutta Metro, as a new metro system and as part of Indian Railways, will have to demonstrate it has given more than due consideration to the threat from CBR agents. No doubt, it has been and is still on the agenda for the Calcutta Metro. To what extent is this threat real from terrorists, terror criminals and extortionists is a matter for local debate, but one constant is true. In the event of an incident, the metro system concerned will be found culpable if reasonable steps have not been implemented to address the risks of a CBR attack.

The above has been said, noting a statement made by Dr. Bruce Hoffman, Director RAND Office Washington DC. Dr. Hoffman is a leading authority in Terrorism and formally the head of the Department of International Relations and Director of the Centre for the Study of Terrorism and Political Violence at St Andrews University in Scotland.

"Total number of attacks are down from a decade ago, but the percentage of people killed is rising. Terrorists are less active but they're much more lethal. There is an identifiable trend that they are deliberately setting out to kill people - a trend that will be reinforced as they gain access to ever more powerful weapons.[7]"

Alphus Hinds founded CyberRisk in 1998 and has since operated as Principal Risk Adviser specialising in applying strategic risk based techniques for the protection of critical infrastructure, information and public safety. He can be contacted at alphushinds@hotmail.com.

7 Reuterlinkextra, Terrorism - The Nuclear Threat

Security in Universities and Colleges

Andrew Cormack

Universities have used Wide Area Networks (WANs) for more than 20 years. My own experiences stretch back to the late 1970s and connections running at the then impressive speeds of 4800 or 9600 bits per second. These were connections running between individual 'mainframes' at universities across the country: at that time there were no desktop workstations or Local Area Networks (LANs) to connect to them. Access to and from the networks was therefore controlled by the individual networked computers. This contrasts sharply with the later arrival of WANs into businesses, most of which had developed extensive internal LANs by this time. Here it was more appropriate to implement controls at the point of entry of the network into the business, using firewalls and proxies. Although university networks have changed greatly since the early days, with pervasive LANs and a national network backbone running at 2.5Gbits/s, access controls are still mainly implemented on local servers rather than on network devices. Staff and students expect to log on to a local server and then have relatively unrestricted access to local and external networks. In business it is more common for access to the LAN to be relatively free, but for wide-area and Internet access to require closely guarded authentication.

Another reason why the university model is more appropriate to education is the different user community. In business most, if not all, local users will be employees of the organization and therefore be well intentioned towards it or, at least, under threat of sanctions if they misbehave. These users can usually be trusted with relatively open local networks, in their own self-interest. In universities and colleges, by contrast, the majority of users will be students, whose shared interest with the organization is much less clear. After examinations, in particular, some may feel they have reason to be actively hostile to the organization whose network they use. A network design that relies primarily on controls implemented at the perimeter of the organization misjudges the threat from these internal users. Worse, it is not even likely to permit any monitoring of their activities that might provide early warning of problems.

Of course education networks should also implement some controls at the network perimeter, but this is more likely to be designed to protect against attack from outside the organization rather than to control internal users. Any computer accessible from the Internet is now subject to continuous external attacks; such is the volume of hostile activity on the Internet. The vast majority of these will be random, automated, generic attacks, like the Nimda worm, rather than being specifically targeted at a particular computer or organization, so defenses in the form of patches or configuration changes are well-known and usually simple to implement. However it makes sense to use perimeter defenses to reduce the number of internal machines exposed to these attacks by hiding their presence from the Internet. Simple blocking of traffic except to specified IP address ranges can be very effective and can often be implemented on existing routers. Such defenses allow effort to be concentrated on protecting the few machines, such as web and mail servers, that must be visible from the Internet to perform their function.

User policies are an important way to encourage good behaviour and punish bad. The JANET network, which connects universities, colleges and research council organizations to each other and to the rest of the Internet, has an acceptable use policy (http://www.ja.net/documents/use.html), which sites connected to JANET are required to enforce on their own local users. Enforcement may take the form of warnings, interviews, loss of access to computer systems or formal disciplinary hearings, and it is in a site's best interest to ensure that these are effective. Many sites also have their own policies, which may be enforced by policing or by traffic filtering. The JANET Security Policy (http://www.ja.net/documents/JANET_security_policy.html) requires sites to take preventative security measures and to assist in the investigation of any security incident. Where problems occur, individual machines or whole organizations can be temporarily or permanently disconnected from the JANET network by the central Network Operations and Service Centre if required to protect other users of the network.

For advice and assistance in preventing or investigating security incidents, sites connected to JANET can call on the network's Computer Emergency Response Team, JANET-CERT. The team provides advice on prevention through its web site (http://www.ja.net/CERT/) and new information and summaries of threats are sent by e-mail to security contacts at every site on the network. When security incidents occur, the team works with affected sites, the Network Operations and Service Centre and other computer security teams to determine the nature of the problem, to trace its cause (if possible), to limit the impact on other sites and to help those affected to regain control of their systems and recover from the incident. JANET-CERT also acts as a central reporting point for problems with organizations within its constituency.

A typical university or college will therefore have a multi-layered approach to security. User behaviour should be guided by policies with effective enforcement; access to internal systems should be controlled, with accounting and other protection against local misuse; perimeter defenses should be used to reduce the exposure to external attack. Each of these measures should be monitored and an effective response made to any problems. Such systems have proved to be effective in reducing security problems while maintaining the open access to computers and networks that educators expect. In a recent survey the ac.uk domain served by the JANET network had the lowest proportion of insecure mail systems; the rate of virus infections is also very low. In the rest of the networking community, JANET is highly regarded, being the source of few problems and dealing promptly and effectively with those that arise. Of course incidents still occur and we will always be working to improve our systems to prevent and respond to these. However with a multi-layer security model it is possible to provide an acceptably secure service even in this challenging environment.

Andrew Cormack is Chief Security Advisor, JANET-CERT, a team he has led for the past three years. Before that he managed computer systems at Cardiff University and on board scientific research ships, giving him very direct experience of the problems and pleasures of providing computer services to academics and students. His main concern is to promote responsible use of computers, both nationally and internationally. He can be contacted at JANET-CERT, UKERNA, Atlas Centre, Chilton, Didcot, OX11 0QS, or email A.Cormack@ukerna.ac.uk

Event Reports

Internet Security

and Intrusion Detection Systems

Rupert Kendrick reports on IRMA's January event which focused on the strategic and operational implications of deploying Intrusion Detection Systems

About 80 delegates packed into the elegant rooms of the Royal Aeronautical Society in London for this event. Although many of the speakers unashamedly admitted to a 'techie' approach to the subject, they made their points with clarity and good humour. As a result, it was possible to absorb – then understand – and even retain – a good deal of complex information relatively easily.

Mark Osborne, Director of Security Engineering, KPMG, opened the conference with a boisterous and cogent presentation. He looked at the limitations of a basic firewall configuration and demonstrated in simple terms how an effective Intruder Detection System (IDS) can complement and reinforce firewall deployment. With a useful comparison between the physical and digital world, he explained that although a firewall may be effectively configured, the content may be insecure, giving rise to damage to reputation, as well as regulatory consequences. He gave examples of the MSDAC hack; the Unicode hack; the Double-decode hack; and the HTML print hack.

IDS, he claimed provided protection in a number of ways:

- 'Shunning' – temporarily blocking the address at the firewall or router;
- Connection Reset – resetting the connection on both the source and destination;
- User Lockout – providing notification and then locking out the offending user account from the system - particularly appropriate to address the problem of disaffected employees.

He also identified a number of faults with IDS. While the primary role is to monitor and alert, this function must be integrated into the organisation's incident response procedures. Incorrect deployment is also a common fault. IDS must be deployed where the network traffic is passing so that anomalies are identified. Of course, any IDS must be tailored to the profiles of the host computer, or the network on which it is installed so that it can identify attack signatures adequately. Finally, it must be remembered that security is a 24/7 function and must have management systems in place accordingly.

Kenneth De Spiegeleire of Internet Security Systems followed with an examination of trends in Internet threats and IDS. He described recent vulnerabilities and gave practical examples of the use of IDS to detect and counter attacks. He opened with some startling statistics – 'by 2002, approximately 19 million people worldwide will have the skills to mount a cyber attack' Vulnerabilities are increasing – all technologies suffer from vulnerabilities and possible mis-configurations. The evidence is that incidents are still penetrating systems and actually peaking some three months after release of an available patch.

Moving on to look at the architecture of present and future IDS, he distinguished between network-based and host-based IDS. The former uses four common techniques to recognise attack signatures: pattern; frequency; correlation of minor events; and statistical anomalies.

Host-based IDS typically monitor system events and security logs, checking files and executables for unexpected changes, while advanced solutions can listen to port activity and alert administrators when specific ports are accessed.

Whilst the first and second generation IDS are based on pattern matching and file integrity and threshold checking, the sheer volume of computations (he gave an example of 720 billion calculations per second) allied to the need for detection accuracy give rise to issues of accuracy, reliability and management capability.

The next generation of IDS will, he claims, include the capability for protocol analysis and parsing mechanisms, which can analyse attack strings with all possible variations. This solution will permit increased performance and accuracy, and be less susceptible to anti-evasion techniques as well as requiring fewer resources.

Tim Pickard, Strategic Marketing Director of RSA Security explained 'Why Passwords are not enough' – providing ample evidence that passwords are inadequate for modern applications which require stronger security solutions. Setting the scene with the required infrastructure for trusted business services, he identified four requisites: authentication (to identify users); access management (to manage access); encryption (to protect the integrity of information); and digital signatures (to protect the integrity of the transaction).

Passwords, he claimed, can be difficult to use. Between 20% and 50% of help desk calls are password related. The use of passwords presents a number of shortcomings:

- users have poor memories and passwords are easily forgotten;
- 50% of passwords are related to users' families;
- Passwords are changed with insufficient frequency;
- Passwords are easy to guess;
- Passwords are frequently written down;
- Work and personal passwords are frequently interchanged.

In addition there are a number of technology solutions, which can now 'sniff' out passwords. Password 'dictionaries' can attempt password cracking at the rate of a million per

second, and one example given was that of 50% of passwords in a user group of 10,000 being 'cracked' in 20 minutes.

RSA, he said, recognised certain elements for true user authentication. The solution must embody 'something you know, and 'something you have' – in other words, something unique about the user, for instance, fingerprint, iris, or voice.

The most recently developed RSA solution embodies a PIN and a token (which includes a multi-digit code), which when entered in the PC is recognised by the server. Delegates were shown an example of the token which in many respects resembles a key fob.

The day ended with a presentation from ***Michael van Strien, Head Penetration Tester, KPMG,*** whose theme was that defence is only as strong as its weakest point, so requiring a comprehensive approach. Continuing the analogy of the physical and digital world, he identified some critical success factors. These included, multiple layers of protection; the use of multiple technologies and the need to integrate these with human resource and management functions.

In a useful comparison between the physical and digital, he claimed that the firewall represented the key and lock; the activity log represented the security camera; the IDS represented movement sensors; the security technician represented the security guard and the digital asset to be protected represented the physical asset.

In a helpful analysis of common faults, he identified the following:

- *Routers:* access lists incomplete or incorrectly applied; unrestricted terminal access to the Internet;
- *Firewalls:* inadequate rules or configuration; inadequate consideration of error logging; changes to configuration not logged; no reporting of authorisation failures;
- *Web servers:* SSL not enabled; critical data in the DMZ; protection only by simple (default) passwords; operating systems not properly configured;
- *Applications:* confidential screens unencrypted; passwords used for high value transactions; unchecked application authorisation; inadequate application logging or alerting;
- *IDS:* focus on known attacks rather than anomalous traffic; inadequate updating mechanisms; incorrect deployment.

At the end of a challenging but rewarding and valuable day, the general feeling of the delegates was that a considerable learning curve had been encountered. The problem with events of this type is that, in the face of such daunting expertise, there is an inevitable feeling of inadequacy and an insurmountable workload involved in matching up to expectations!

The Subversive Spreadsheet

IRMA Event, 12 February 2002

Journal Events Reporter, Rupert Kendrick, reports on an IRMA event in February, which examined how spreadsheets can undermine an organisation's business performance

This seminar brought a full house at the offices of KPMG, for, what is generally considered to be, a rather dry subject. It proved to be quite the opposite in the hands of David Chadwick, Senior Lecturer at the University of Greenwich and Grenville Croll of Andersen Business Modelling Group. Between them they have formed the European Spreadsheet Risks Information Group – readers are recommended to visit the web site at www.eusprig.org

David Chadwick opened with a lively presentation and an amusing quotation that spreadsheets are like children at Christmas – 'anxious to get on with the games and not to think about the rules'. He then unveiled illustrations of a catalogue of errors that commonly arise in spreadsheets in many organisations, in many cases, without any awareness. These include errors in respect of: software; users; formatting; logic; data input; planning; decision-making; as well as numerous others.

Procedurally, errors arise through inappropriate application of wizard functions; incorrect sorting procedures; software malfunction and auditing and accounting procedures. According to some statistics, 70% of spreadsheets had no quality assurance. He then discussed methods of developing a spreadsheet model. This involved the need to address: client requirements; analysis of information; design considerations, implementation; and review. There are various audit tools available, such as Microsoft; Spreadsheet Professional; Spreadsheet Detective; Operis Analysis Kit and Spreadsheet Auditing for Customs & Excise (SPACE).

Grenville Croll explained how Andersen approach the task of auditing and provided an introduction for a Model Review. The process involves employing a proprietory tool for assessing risk, decomposing the model and feeding the findings into an 'Inference Engine'.

The review model was illustrated in the form of a pyramid. Level one (the base level) involved checking: model maps, code reviews, range names, queries and responses. Level two involved: a higher-level review; documentation checking; and analysis and comparisons. Level three involved: checking specific sensitivities and measuring the model against certain contingencies. The final levels involved a final review and the supply of a report to the client.

Spreadsheets are frequently overlooked in the context of information assurance and overshadowed by the hype of Internet technologies. This seminar proved that their potential for causing problems should not be underestimated.

Rupert Kendrick is a lawyer, freelance editor and law management specialist who publishes his own newsletter Cyber-risks News. His book Managing Cyber-risks is being published by the Law Society later this year. He can be contacted at RupKendrick@aol.com

The Web Page

Finding a cure for the ISISTS syndrome

Andrew Hawker

University of Birmingham

Most of us have had the experience of half-remembering a news story from some days or weeks ago, which suddenly seems very relevant to something which has come up for discussion. This might be described as the "I'm sure I saw that somewhere… " syndrome. The trouble usually is that you have no idea when or where you came across the item in question. Somebody, somewhere, reported on flaws in SNMP or a Valentine's Day virus. But where?

There are now dozens of Internet sites that offer news on IT topics. Many of these have sections or threads which deal specifically with security and control. However, they vary considerably in their objectives. Some aim to provide "hot" news, with tabloid-style headlines and an emphasis on dramatic stories. Others provide more considered coverage, and in some cases have archives going back several years.

Searching the wrong kind of site can be a frustrating experience. In general, the sites with eye-catching headlines and up-to-the-minute reports are often the most difficult to search, and can be disappointing when it comes to details and cross-references. Perspectives can vary, too. Some sites are very technical and product-centred, while others concentrate more on the management and business issues.

This column reviews some of the sites that offer services that are free of charge. There are some excellent web sites and electronic newsletters for which subscriptions are payable, but this column is staying with its usual miserly instincts.

The majority of free news sites are American, which is no particular problem, given the many issues that revolve around US products and companies. Some sites are "clusters", so that it pays to go to the central site if you want the widest possible range of material. For example, **IDG.net** is a hub site for a dozen or more different publications, including **Computerworld**, **PCWorld** and **ITWorld**. At first sight, this seems a good way of hunting through several publications, but unfortunately the advanced features of the search engine did not seem to be working properly at the time of visiting. **TechWeb** is another cluster site that embraces **InformationWeek**, **InternetWeek** and **Network Computing**.

These sites tend to be "techie" in their emphasis, as is **eWeek**, which is written very much for IT industry "insiders". (For example, it runs online opinion surveys on questions such as: "Is an embedded SQL engine important to the future of Windows?") A search on "audit" is likely to come up with articles on software piracy, rather than more mainstream questions of computer audit. Possibly even more technical is the **Engineering News-Record**, which provides short, readable articles on IT, but is quite likely to drop in a detailed circuit diagram just to throw you. Relatively few of its articles deal with security.

More general coverage is provided on the cluster of sites operated by **NewsFactor**, particularly in the **Ecommerce Times**. However, the sites do not have a particular "security" thread, and you are presented with a fair amount of advertising and sponsorship messages. The feel of these sites is similar to that of the UK's own Silicon.com. This site has undergone some reorganisation over the past few months, and security is no longer one of its main categories. However, if you look in the "Systems and Development" zone, there are a couple of threads concerned with security. **Silicon.com** also provides much better coverage of stories arising in the UK and Europe.

Many sites have been set up by publishers who are already well established in the old-fashioned print media. The Washington Post, for example, runs the **Newsbytes** site, which contains a good collection of topical articles, with some useful references and hyperlinks. However, only a small minority of the stories deal with security issues, and these can be difficult to hunt down. In this country, **Computer Weekly** is always a good source of reference, particularly if you want to go further back in time. It has an Advanced Search option which is convenient to use, and which works well. Articles from the weekly journal **Computing** can be found via the **VNUNet** site. This includes other articles sourced by VNU, and there are some clearly indexed security headings to choose from.

In the United States, **Infoworld** has a web site with a security thread. The articles are peppered with hyperlinks, some of which are of only marginal relevance or interest. Another established print magazine is **Computerworld**, (mentioned previously as part of the IDG cluster). This carries an archive of the recent printed editions by date, which can be helpful if you are already reasonably sure of the timing of the story you are looking for.

Finally, there are some companies involved in IT security who offer indexing of current articles, with hyperlinks to other on-line sources. An example is **@Stake** in the US, which tracks relevant stories in a variety of American and Canadian publications. Progress is sometimes slow, as the cross-links can take several seconds to activate, but it does provide a much broader view of events than elsewhere.

URL's for the sites mentioned above are:

@Stake	www.atstake.com
Computer Weekly	www.cw360.com
Computerworld	www.computerworld.com
Ecommerce Times	www.ecommercetimes.com
Engineering News-Record	www.enr.com
eWeek	www.eweek.com
IDG	www.idg.net
Information Week	www.informationweek.com
Infoworld	www.infoworld.com
Internet Week	www.internetweek.com
ITWorld	www.ITWorld.com
Newsbytes	www.newsbytes.com
PCWorld	www.PCWorld.com
Techweb	www.techweb.com
VNU	www.vnunet.com

IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

THE ANNUAL GENERAL MEETING

of the

INFORMATION RISK MANAGEMENT & AUDIT GROUP

of

THE BRITISH COMPUTER SOCIETY

to be held on

TUESDAY 14 MAY 2002 at 16.00 (immediately before the members' meeting)

at KPMG'S offices, 8 Salisbury Square, London, EC4Y 8BB

AGENDA

1. Approval of the minutes of the AGM held on 15 May 2001
2. Chairman's Report
3. Treasurer's Report
4. Election of Officers
5. Election of Honorary Auditor
6. Appointment of Committee
7. Plans for 2002/2003
8. Any other business

The meeting will precede the members' meeting on Data & the Law.
There is no charge for attendance at the AGM which is open to all IRMA members irrespective of whether or not they attend the members' meeting on the day.

Notice of the Annual General Meeting of the Information Risk Management & Audit Specialist Group of the British Computer Society (IRMA)

The AGM for 2001/2002 will take place on Tuesday 14 May 2002 at KPMG's office, 8 Salisbury Square, London, EC4Y 8BB, immediately before the afternoon's members' meeting on Data & the Law.

An Agenda for the meeting is shown opposite. There is no charge for the meeting or the AGM which are both open to all IRMA members. Members may attend the AGM irrespective of whether or not they attend the members' meeting.

Nominations for the Management Committee

As usual at this time, we are seeking nominations for the Group's Management Committee. We hold about 4-6 committee meetings a year, usually held at the end of Technical Briefing, or scheduled as needed at other times during the year. Each committee member is allocated a specific role and the Committee is assisted by an Administrator. The Committee is not a 'clique' and we would very much welcome new people, new ideas and lots of enthusiasm! Names of the current Committee Members are given below.

If you would like to discuss any committee posts please contact Raghu Iyer, Secretary, or any other committee member whose details are given in the Journal.

Please do not be concerned if a position is not currently vacant, just apply using the nomination form below.

THE CURRENT MANAGEMENT COMMITTEE

Chairman	John Bevan	Consultant
Deputy Chairman (Temp. post)	Siobhan Tracey	Booker plc
Secretary	Raghu Iyer	KPMG
Treasurer	Mike Demetriou	Consultant
Journal Editor	John Mitchell	LHS Business Control
Membership Secretary	Jenny Broadbent (Resigned during 2001/2002)	Consultant
Meeting organisers	Peter Murray	Consultant
	Paul Plane	Dai-Ichi Kangyo Bank
	Rosemary Mulley	Nabarro Nathanson
	Pete Biss	John Lewis Partnership
Marketing	Steve Pooley	Consultant
Academic Relations	David Chadwick	Greenwich University
Webmaster	Allan Boardman	Goldman Sachs

THE BRITISH COMPUTER SOCIETY

INFORMATION RISK MANAGEMENT & AUDIT SPECIALIST GROUP (IRMA)

Nominations for the 2002/2003 Committee

Position: .....

Nominee: .....

Proposer: .....

Seconder: .....

Signature of Nominee agreeing to serve on the Committee ..... Date: .....

HUMOUR PAGE

Contributed by Paul Plane

"Very funny, Scotty. Now beam down my clothes."

Friends help you move. Real friends help you move bodies.

The gene pool could use a little chlorine.

We are born naked, wet and hungry. Then things get worse.

Make it idiot proof and someone will make a better idiot.

I'm not a complete idiot, some parts are missing!

He who laughs last thinks slowest!

Always remember you're unique, just like everyone else.

Give me ambiguity or give me something else.

A flashlight is a case for holding dead batteries.

Lottery: A tax on people who are bad at maths.

There's too much blood in my caffeine system.

Learn from your parents' mistakes - use birth control!

Puritanism: The haunting fear that someone, somewhere may be happy.

Consciousness: that annoying time between naps.

I used to have a handle on life, then it broke.

Don't take life too seriously, you won't get out alive.

I don't suffer from insanity. I enjoy every minute of it.

Better to understand a little than to misunderstand a lot.

Change is inevitable, except from a vending machine.

"Criminal Lawyer" is a redundancy.

Out of my mind. Back in five minutes.

Laugh alone and the world thinks you're an idiot.

Your kid may be an honour student but you're still an IDIOT!

When you do a good deed, get a receipt, in case heaven is like the Inland Revenue.

I took an IQ test and the results were negative.

When there's a will, I want to be in it!

Okay, who stopped the payment on my reality check?

Time is the best teacher; unfortunately it kills all its students!

It's lonely at the top, but you eat better.

Warning: Dates in a calendar are closer than they appear.

We are Microsoft. Resistance Is Futile. You Will Be Assimilated.

Be nice to your kids. They'll choose your nursing home.

Why is "abbreviation" such a long word?

Ever stop to think, and forget to start again?

2 + 2 = 5 for extremely large values of 2.

3 kinds of people: those who can count & those who can't.

I'm a corporate executive — I keep things from happening.

On the other hand, you have different fingers.

Back Up My Hard Drive? How do I Put it in Reverse?

I just got lost in thought. It was unfamiliar territory.

Seen it all, done it all, can't remember most of it.

Those who live by the sword get shot by those who don't.

I feel like I'm diagonally parked in a parallel universe.

He's not dead — He's electroencephalographically challenged.

You have the right to remain silent. Anything you say will be misquoted, then used against you.

I wonder how much deeper the ocean would be without sponges.

Honk if you love peace and quiet.

Despite the cost of living, have you noticed how it remains so popular?

Nothing is fool-proof to a sufficiently talented fool.

A day without sunshine is like night.

All those who believe in psychokinesis, raise my hand.

I almost had a psychic girlfriend but she left me before we met.

If everything seems to be going well, you have obviously overlooked something.

Support bacteria - they're the only culture some people have.

Shin: a device for finding furniture in the dark.

Many people quit looking for work when they find a job.

If I worked as much as others, I would do as little as they.

When I'm not in my right mind, my left mind gets pretty crowded.

I used to have an open mind but my brains kept falling out.

I couldn't repair your brakes, so I made your horn louder.

For every action, there is an equal and opposite criticism.

No one is listening until you make a mistake.

Success always occurs in private, and failure in full view.

The colder the X-ray table, the more of your body is required on it.

The hardness of the butter is proportional to the softness of the bread.

Two wrongs are only the beginning.

You never really learn to swear until you learn to drive.

The problem with the gene pool is that there is no lifeguard.

Monday is an awful way to spend 1/7th of your life.

Bills travel through the mail at twice the speed of cheques.

BCS MATTERS!

Colin Thompson
BCS Deputy Chief Executive

Colin Thompson, BCS Deputy Chief Executive, reviews some of the current BCS news items. Further information on these or any other BCS related issues may be found on the BCS Web site ("http://www.bcs.org.uk/")

Information is also available from Customer Services at The British Computer Society, 1 Sanford St, Swindon SN1 1HJ (e-mail to marketing@hq.bcs.org.uk)

Forums get to work on key issues

The three new BCS Forums, launched at the end of last year as part of a major BCS reorganisation, have started to set their agendas after identifying key issues at the initial meetings of their Management Committees – and they now want both BCS members and non-members to get involved.

The ENGINEERING AND TECHNOLOGY FORUM has set out as its main initial theme the challenging issue of why major information systems projects fail.

There is considerable evidence that only a small percentage of major software projects succeed, in the sense of delivering what was expected, roughly to time and to budget. Whilst there is consensus on the symptoms of the problem there has been less of a coherent view on the underlying causes of the problems, and on potential solutions.

The Forum now wants to help address this problem by trying to clarify the fundamental causes of project failures and to address aspects of the problem that are within The BCS' sphere of responsibility.

The MANAGEMENT FORUM is keen to initiate work on management competences, using the existing *Industry Structure Model*, The BCS' set of standards for IS roles, and the *Skills Framework for the Information Age*, which is managed by the e-skills National Training Organisation. It believes that these could be developed and promoted by the Forum as a competence framework for both individuals and employers.

In addition the Management Forum has begun to develop a model of career paths and advancement which it feels could be applied to all aspiring IS managers. It could also complement initiatives from other organisations, such as the Cranfield and Henley management schools.

The EDUCATION AND TRAINING FORUM has identified issues in all education sectors which it wants to start addressing. These include staff development, investment in further education, e-learning skills, lifelong learning and development awards recognition. These will be given priorities and taken forward over the coming year.

More information, and an on-line registration facility can be found at www.bcs.org/forums.

Implementing BCS Web enablement

User acceptance testing is in progress for a major enhancement to the BCS Web capability. The Web Enablement programme has been running for the past year with the aim of improving the standard, availability and relevance of our services to membership, to provide new opportunities for the Society and improve our operational efficiency. More specifically, the objectives are to:

1. Provide a Members' Extranet that will allow members to update the contact details we hold on the Genesis membership database, allow on-line payment of subscriptions and enable additional web-based services.
2. Re-develop the existing BCS web site to enhance its use as a strategic marketing tool.
3. Provide a higher level of support to the Branches and Specialist Groups to enable better administration and promotion of their activities
4. Develop additional services such as on-line testing and a Virtual Career Logbook
5. Provide a sophisticated e-mail service for members and to enable better low-cost promotion of our services to members and non-members electronically.

For Specialist Groups the programme will provide a range of new support services, including:

- The ability to hold SG members on the Genesis database and to update the contact details of individuals on-line
- On-line access to modern e-mail list server facilities, with addresses updated automatically from the Genesis database;
- Access to a series of on-line reports, specific to individual groups, updated instantly on demand from the Genesis database;
- Access to a web-based knowledge management system with built-in security
- The use of a Web-based threaded discussion group tool;

This is a long-term development programme between the Society and Ramesys professional Services, the company that supplies the Genesis database and the associated application systems. Subject to successful user acceptance testing we expect to start rolling out the facilities mentioned above between April and June of this year. However, this is only the first stage of a longer-term programme and future developments will include facilities for Internet trading, reservations for conferences and seminars and support for the SG subscription renewal process.

A new Code of Conduct for BCS members

A revision of the Code of Conduct has been approved by the BCS Council. The previous version had remained unchanged since 1992, and the opportunity has now been taken to make a few small but significant changes. These include the insertion of some

explanatory information and interpretation of some of the clauses.

The revised Code took effect in January and a copy can be downloaded from http://www.bcs.org/codes. Printed copies are available from assistant registrar Mandy Bryer via mbryer@hq.bcs.org.uk and 01793 417482.

BCS Fellow wins top women's engineering award

Beth Hutchison, a BCS Fellow at IBM has become the first person in IT to win the annual Karen Burt Award, named after an eminent physicist who died young in 1997. The award is presented by the Women's Engineering Society, for commitment to promoting the profession. Beth works on Java at IBM, where she is also head of the women's leadership team and a mentor to seven software engineers with technical leadership potential.

This is the second major award for a female BCS Fellow in recent months: Mandy Chessell, also from IBM, where she is a middleware specialist and one of the company's 'master inventors', recently became the first woman to win one of the four annual silver medals from the Royal Academy of Engineering. These are presented for outstanding contribution to engineering.

BCS members urged to help with BS 7799 update

The BS 7799 standard Specification for Information Security Management Systems - now also the basis of an international standard - is being updated, and BCS members are being urged to take part by commenting on the new draft.

The draft for public comment has just been released, and the comment period runs until 31 March 2002. Copies of the draft are available from via the C-Cure Web Site (www.c-cure.org) at £10 for subscribing BSI members, £20 for others.

NHS Adopts ECDL as standard

The UK National Health Service is adopting the European Computer Driving Licence user skills qualification as a standard for its entire 700,000 staff.

The initiative is aimed at giving everyone from porters to senior medical consultants the chance to increase familiarity with IT and gain an internationally recognised qualification - and it is also being linked to another NHS project, Clinician Connect, which aims to give access to a computer with Internet access to all clinical staff this spring and all other staff in the next year.

The significance of the ECDL decision is reflected in the fact that it was announced by health secretary Lord Hunt.

Well over 300,000 people have gained or started working for the ECDL in the UK alone since The BCS launched it in May 1998. Worldwide there are well over 1.6 million candidates in more than 55 countries. Other big organisations adopting it as a standard range from IBM to the Ministry of Defence and the Bank of England.

Details are at http://www.ecdl.co.uk

University crisis highlighted by BCS study

A serious staffing problem in UK University computing departments has been highlighted by a survey by The BCS with the Conference of Professors and Heads of Computing (CPHC) and market research organisation Metra Martech. The study gives the fullest view ever achieved, with 67 out of 100 institutions completing the questionnaire - and provides clear evidence of a range of staffing problems.

Staff are mostly aged 35-54. Over 90% of departments have unfilled positions, with 13% reporting at least 20% unfilled positions. Student-staff ratios are significantly higher than the 12-1 norm, with 30% exceeding 30-1. Almost 75% of respondents say working conditions have got worse in the last five years.

Issues include workload, bureaucracy and career prospects, with academic salaries seen as the major impediment.

Representations have been made to politicians, and in November BCS Judith Scott and Ian Watson, the Chair of CPHC met with higher education minister Margaret Hodge. Their message to her was very clear – 'The UK is in grave danger of losing its competitive edge. This is not a problem that can be ignored; the risks are far too great. In 20 years we could have computing departments with no staff.'

IT Consultants get their own Specialist group

A new specialist group for internal and external IT consultants is being formed by BCS. The new group aims to promote best practice, ultimately to the benefit of both IT people and users. It will do this by liaising with academic institutions and other professional bodies to develop best practice; facilitating the sharing of information, notably through events, some with similar bodies; and promoting The BCS' Information Systems Examinations Board's new Certificate in IS Consultancy Practice.

Membership of the Consultancy Specialist Group is open to anyone interested in consultancy, whether they work in consultancy practices large and small, as sole practitioners, or as internal consultants in companies or the public sector.

Further details of the new group are available from Rajan Anketell (rajan@anketell.com). Information on the ISEB certificate is at http://www.iseb.org.uk/conskills

And Finally…….

News of the new BCS Chief Executive.

I mentioned in the last edition of this newsletter that Judith Scott, BCS Chief Executive for the past 6 years, had decided to retire later this year. In February, following an open recruitment competition, the Society announced that she would be succeeded by David Clarke.

David is 53. Until recently he was Chief Executive of Trinity Mirror Digital Media. He was recruited by Mirror Group in 1999 to develop that company's digital media business, but

the acquisition of the Mirror Group by Trinity resulted in a change of strategy, and David is now completing the sale of the individual businesses within the Digital Media subsidiary. He is also writing a book on Internet developments over the past five years.

Previous to that, David was Chief Executive of Virgin.net and, earlier, UK managing director of Netcom Internet. He took on these challenging ISP roles after an extensive senior level career in marketing for technology companies. He was marketing director for Compaq for several years and, before that, Marketing manager for Hewlett Packard and then Digital Equipment Co. His earlier experience was on the finance side of some smaller companies. He hoped originally to be a professional footballer, and joined Leeds United when he left school, but injury put paid to that ambition.

David will join the Society on 1 May 2002 at the beginning of the new financial year. Following the handover period, Judith will be working with the Honorary Officers on one or two specific projects prior to her retirement at the beginning of October.

THE BCS INDUSTRY STRUCTURE MODEL

Malcolm Sillars

BCS Professional Director

ISM EXPANDS SCOPE AND VALUE WITH COMMS UPDATE

Five new job functions have been added to The BCS' Industry Structure Model (ISM), the internationally recognised set of training and development standards for IT specialists, following an extensive review by the UK Communications Managers Association.

Version 3.3 of the ISM will be available from the end of February with the additions of client services management, installation and implementation, network design, network operations, and safety engineering.

At the same time the systems integration function has been substantially expanded, and major updates have been made to a further seven functions, including network planning, telecommunications management and project management.

The work by members of the Communications Managers Association is part of the aim to extend the ISM to the whole information and communications technology area.

The review also extends the ISM's support for The BCS' Information Systems Quality at Work scheme, which gives public recognition to employers that demonstrate commitment to best practice in IT staff development. Organisations that achieve the Information Systems Quality at Work standard typically use the ISM to underpin their planning and career development. The ISM has been maintained by The BCS since 1986. The paper version was superseded by an electronic version, release 3, 1996. More than 150 professionals have worked on release 3 and its other updates in 1997 and 1999. The ISM describes around 260 roles in and the activities, qualifications and training at up to 10 different levels in each role. This is likely to be the last update to release 3, as we have already started planning release 4, which should be available in 2003. Full information on the ISM is at www.bcs.org/ism.

IRMA
INFORMATION RISK MANAGEMENT & AUDIT

◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	John Bevan	Audit & Computer Security Services	01992 582439
Designate*	Peter Biss		john_bevan@ntlworld.com
SECRETARY	Raghu Iyer	KPMG	020 7311 1412
Designate*	Siobhan Tracey		raghu.iyer@kpmg.co.uk
TREASURER	Mike Demetriou	CrestCo Ltd	020 7849 0000
Designate*	Jan Lubbe		mike.demetriou@crestco.co.uk
MEMBERSHIP SECRETARY	Celeste Rush		RushLSE97@aol.com
JOURNAL EDITOR	John Mitchell	LHS Business Control	01707 851454
			john@lhscontrol.com
WEBMASTER	Allan Boardman	Goldman Sachs	07881 930814
			webmaster@bcs-irma.org
SECURITY COMMITTEE LIAISON	Peter Biss		pete_biss@hotmail.com
MEMBER SERVICES BOARD LIAISON	Celeste Rush		RushLSE97@aol.com
EVENTS	Siobhan Tracey	Iceland plc	Siobhan.Tracey@booker.co.uk
	Alex Brewer	Lloyds TSB	alex_brewer@bigfoot.com
	Steve Pooley	Independent Consultant	01580 891036
			steve.pooley@lineone.com
	Rosemary Mulley	NabarroNathanson	0118 950 5640
			r.mulley@nabarro.com
	Darren Kempson		
ACADEMIC RELATIONS	David Chadwick	Greenwich University	020 8331 8509
			d.r.chadwick@greenwich.ac.uk
LOCAL GOVERNMENT LIAISON	Peter Murray		01992 582105
			cass@peterm.demon.co.uk

* To be ratified at the AGM

Membership Enquiries to:

Janet Cardell-Williams
49 Grangewood
Potters Bar
Herts EN6 1SL
t: 01707 852384
f: 01707 646275
e: members.irma@bcs.org.uk
www.bcs-irma.org

IRMA
INFORMATION RISK MANAGEMENT & AUDIT
◆ A SPECIALIST GROUP OF THE BCS ◆

BCS
THE BRITISH COMPUTER SOCIETY

Membership Application

(Membership runs from July to the following June each year)

I wish to APPLY FOR membership of the Group in the following category and enclose the appropriate subscription.

CORPORATE MEMBERSHIP (Up to 5 members) * £75

* Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal *(see over)*

INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)* £25

INDIVIDUAL MEMBERSHIP *(A members of the BCS)* £15

BCS membership number: _____

STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment).

Educational Establishment: _____ £10

Please circle the appropriate subscription amount and complete the details below.

INDIVIDUAL NAME: (Title/Initials/Surname)
POSITION:
ORGANISATION:
ADDRESS: POST CODE:
TELEPHONE: (STD Code/Number/Extension)
E-mail:
PROFESSIONAL CATEGORY: (Please circle) 1 = Internal Audit 4 = Academic 2 = External Audit 5 = Full-Time Student 3 = Data Processor 6 = Other (please specify)
SIGNATURE: DATE:

PLEASE MAKE CHEQUES PAYABLE TO "BCS IRMA"AND RETURN WITH THIS FORM TO

Janet Cardell-Williams, IRMA Administrator, 49 Grangewood, Potters Bar, Herts EN6 1SL. Fax: 01707 646275

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

1 = Internal Audit	4 = Academic
2 = External Audit	5 = Full-Time Student
3 = Data Processor	6 = Other (please specify)