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

JOURNAL
VOLUME 17 NUMBER 4 WINTER 2007 ISSN 1741-4229

Programme of Briefings & Meetings 2008

Date	***Subject***	***Speaker***	***Time***	***Location***
8 Jan	Data Quality (joint meeting with the Data Management SG)	Keith Gordon	17.30	BCS London Office
5 Feb	Handling computer-related incidents in the workplace	Jan Collie	17.30	BCS London Office
14 Feb	Software auditing (joint meeting with the Advanced Programming SG)	John Mitchell	17.30	BCS London Office
4 Mar	Critical National Infrastructure	TBA	17.30	BCS London Office
1 Apr	Radio-frequency identification (RFID)	Ken Munro	17.30	BCS London Office
27 May	AGM + TBA	TBA	17.00	BCS London Office
10 June	TBA	TBA	17:30	BCS London Office
1 July	Payment Card Industry (PCI) Data Security Standard (DSS)	TBA	17:30	BCS London Office

Apart from some joint meetings with other organizations all meetings will be held at BCS, 5 Southampton Street, London WC2 7HA
This is a draft programme only and is subject to change. For confirmation of dates and further information,
watch the **Journal**, email **admin@bcs-irma.org** or visit our website at **www.bcs-irma.org**

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 delegate's pack.
For venue map see back cover.

Email distribution is here…

IRMA has moved from paper to electronic distribution of the Journal, so we need your email address! If you have not already supplied it, please can you send your email address to our admin office at admin@bcs-irma.org – Many thanks.

Contents of the Journal

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 be by e-mail and 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 electronic digital image.

Submission Deadlines

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

PLEASE NOTE THE EMAIL ADDRESS FOR

IRMA ADMIN IS:

admin@bcs-irma.org

The views expressed in the Journal are not necessarily shared by IRMA.
Articles are published without responsibility on the part of the publishers or authors for loss occasioned
in any person acting, or refraining from acting as a result of any view expressed therein.

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
john@lhscontrol.com

Produced by Carliam Artwork,
Potters Bar, Herts

Editorial

John Mitchell

It has been a bad couple of months for the IT assurance industry. First John Ivinson died and now William List has passed away. Willie, as he was always known to his friends was Chairman of this Specialist Group for a seven year period from 1981 to 1988. I had the honour of following in his footsteps and we often shared conference platforms together. Willie was an innovator of the first order with the ability to cut through the fog and reach the heart of any issue. Together with David Brewer he produced the most important paper on control mechanisms in the last decade which I published in this Journal in June 2005. Willie was a hard drinking and hard smoking auditor of the old school. He wanted answers and was not going to be diverted by devious misdirection. He was also charming and great company. He had a heart transplant some ten years ago and had been living life on borrowed time since then. Apart from the occasional bad day, when his usual intake of thirty-six pills left him without his usual energy, you would never know that he had undergone such major surgery. He had recently sold his house and was about to move and was having great fun sorting through his archives and deciding what to keep – all of it! Willie has a great sense of humour and loved the following story which he recounted with relish when he was illustrating the law of unintended consequences. A young executive was leaving the office late one evening when he found the CEO standing in front of a shredder with a piece of paper in his hand. “Listen,” said the CEO, “this is a very sensitive and important document here, and my secretary has gone for the night. Can you make this thing work?” “Certainly,” said the young executive. He turned the machine on, inserted the paper, and pressed the start button. “Excellent, excellent!” said the CEO as his paper disappeared inside the machine. “I just need one copy”. Willie would roar with laughter and infect the entire audience. I will miss his incisive mind, his big laugh and his wisdom. The IT assurance profession is greatly diminished by his passing.

On the subject of obituaries I am wondering if we are seeing the early death throes of the Basel II minimum capital requirements for banks, especially as the American Federal Reserve are adopting it! The Americans often come late to the international dinner table and it is worth reviewing a quotation from Federal Reserve Board Governor Randall S. Kroszner. “The improvements in risk management under Basel II will be valuable and important in promoting the resiliency of the banking and financial systems”. Really? This is at just the time when I am wondering whether Basel II is worth the paper it is printed on. Basel II did not save Northern Rock and our tripartite supervisory system (Treasury, Bank of England, Financial Services Authority) failed woefully in sorting out the mess. The first run on a British bank in 150 years is hardly an endorsement of Basel II to protect a bank’s liquidity. I am surprised that neither the Bank of England, the Treasury, the Financial Services Authority, nor financial journalists have yet questioned the efficacy of Basel II. Capital requirements rules state that credit institutions must at all times maintain a minimum amount of financial capital, in order to cover the risks to which they are exposed. The aim is to ensure the financial soundness of such institutions, to maintain customer confidence in the solvency of the institutions, to ensure the stability of the financial system at large, and to protect depositors against losses. We have seen from Northern Rock however, that this underlying principle is fundamentally flawed. The determining factor is not so much how much you have, but how much you can borrow and at what rate. So why the big silence from the supervisory big three? Intense embarrassment perhaps?

You may be wondering what Basel II has to do with computer auditing? Well, its risk based approach assumes that you have at least three years good records of your previous losses, so data integrity is a prime requirement. However, doesn’t the FSA keep reminding us that past performance is no guide to the future? Hey, ho, if past performance provides no useful information for dim wits like us to help us select a financial product, what makes it so good for banks when determining their capital reserves? Answers on the back of an envelope please to the Governor of the Bank of England, The

Chancellor of the Exchequer and the Chief Executive of the FSA.

In this issue, we have our usual mix of regular contributors ranging from Bob Ashton's Down Under column, Mark Smith's Member Benefits, a financial update from our Treasurer Jean Morgan and Andrea Simmons of the Security Forum telling us just what a hard working person she is. Not to be outdone, Ross Palmer our Chairman (not a chair you notice), provides a complicated formula to calculate the likelihood of Murphy's law kicking in. As my old friend William List would have said, "if you are not running around like a headless chicken, them you don't appreciate the gravity of the situation". Finally, you will find a missive penned by yours truly dealing with digital forensics.

A happy Christmas to you all and a prosperous, or at least a no redundancies, New Year.

Letter to the Editor

John

Willie was unique and is irreplaceable. I will miss him tremendously, as I am sure we all will.

Having worked with him very closely over the years I can honestly say he was an inspiration. We didn't always agree, but by god he made me justify myself and that has made me a better academic. Though of course in the early 1990s when I was on the wagon he wasn't such a good influence (bless him).

Dr. Rob Melville

IRMA MEMBERS' BENEFITS DISCOUNTS

We have negotiated a range of discounts for IRMA members, see below…

Software

Product	Discount Negotiated	Supplier
Caseware Examiner for IDEA (mines security log files for Windows 2000, NT, XP)	15%	Auditware Systems (www.auditware.co.uk)
IDEA (Interactive Data Extraction and Analysis)	15%	Auditware Systems (www.auditware.co.uk)
Wizrule (data auditing and cleansing application)	20%	Wizsoft (www.wizsoft.com)
Wizwhy (data mining tool)	20%	Wizsoft (www.wizsoft.com)

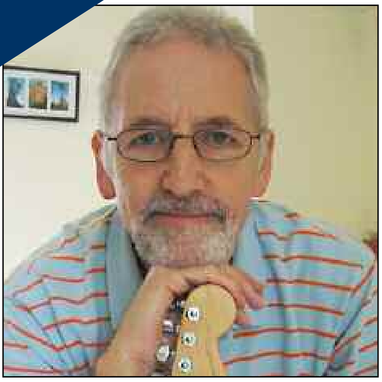
Events

Event	Discount Negotiated	Contact
E-Tec courses (www.e-tecsecurity.com)	10%	Margaret Mason (info@e-tecsecurity.com)
IACON (www.iir-iacon.com)	20%	Jonathan Harvey (jharvey@iirltd.co.uk)
All Unicom events (www.unicom.co.uk)	20%	Julie Valentine (julie@unicom.co.uk)

We are constantly looking to extend this range of discounts to include additional events, training courses, computer software or other products that our members may find beneficial. If you have any suggestions for products we could add to the list, please contact Mark Smith (mark.smith@smhp.nhs.uk), our Members' Benefits Officer, and he will be happy to approach suppliers.

Chairman's Corner

Ross Palmer



Risk Transfer and Northern Rock

Despite warnings about tigers from the indigenous population, two chaps who had been trekking across India decided to take a diversion outside the warden-controlled areas of the local countryside, but for added assurance they took a rifle with them. It was not long before they turned into a jungle clearing and, sure enough, on the opposite side, a mature Bengal Tiger watched them with increasing interest.

The first guy calmly put the rifle to his shoulder, squeezed the trigger and … CLICK!

As the big cat slowly gathered pace towards them, the same chap took out a pair of running shoes from his rucksack, whereupon his astonished and very uneasy colleague said, "What? You can't hope to outrun THAT!"

"My dear chap," he replied, "I only have to outrun YOU."

This excellent story highlights the principles of risk transfer – something we don't hear too much about in risk treatment mythology. Risk transfer has been defined as "shifting risk from one party to another; examples include purchasing insurance coverage or issuing debt".

Normally, transfer of risk is a pre-determined option usually with a hefty premium reflecting the potential hit that may be incurred by the third party taking it on. Take the recent Northern Rock crisis (which, I admit, did see your author in a bit of "panic withdrawal" mode), with the Government providing what is termed "a contingent liability for the purposes of National Accounts and Public Sector Finances".

Richard Murphy, of independent consultancy Tax Research, summed up the risk situation profoundly: "In effect the Chancellor has now given all bank customers a guarantee that, just about whatever their bank does, their money is safe. Much of the risk has gone out of banking as a result and has been assumed by the state". This morning (5 November) on the "Today" programme, John Humphrys put it to the Chancellor that this taxpayers' money has been handed over to the NR Executive to use as they see fit and have consequently lost control of it.

At the time of writing, the NR loan from the Bank Of England stands at £23Bn, or £730 per UK taxpayer. (So, can I please add mine to my remaining NR balance?)

This ostensibly unlimited bail-out, in turn, has led to claims from other organisations, especially on behalf of pensioners hit by collapsed financial institutions, such as Equitable Life, declaring the rules (pardon the pun) inequitable.

So, where do the goalposts for risk transfer get moved to from here?

Murphy's Law

Murphy's Law (which also goes by another name, depending on the school you went to) states that *"things will go wrong in any given situation, if you give them a chance"*.

From a hard copy mailing I received recently, apparently a panel of experts has developed a statistical formula for predicting Murphy's Law occurrences:

$$((U + C + I) \times (10\text{-}S)) / 20 \times A \times 1/(1\text{-}\sin(F/10))$$

(Where U = Urgency, C = Complexity, I = Importance, S = Skill, F = Frequency, A = Aggravation, with each variable rated on a scale of 0 to 9.)

The formula is applied to produce a probability score and the higher the number, the more likely Murphy's Law will occur.

It strikes me (no, I'd better not say that) that this could be a useful appendix to any Business Continuity Plan. If only all corporate risks could be so precisely defined!

The Byron Review

I remember, many, MANY years ago, in response to exhortations from my primary school teachers, offering up the occasional prayer, *"Please God, help me to be good"* and later, in the quiet of my bedroom, with the adjunct, *"… but not just yet"*. Spurred on by the antics of Dennis The Menace and Just William, there was a childlike determination that to enjoy oneself meant just a teeny-weeny bit of devilry, like stretching cling-wrap across the top of the toilet bowl before the arrival of grandparents. (OK, so cling-wrap wasn't invented then, but I wish it had been.)

Sadly, the roles have now become sinisterly reversed with **children** becoming the unwitting targets of malice through exposure to the internet and inappropriate video-gaming influences, so it was particularly interesting to read of the Byron Review, an independent review of the risks to children from these media (see the consultation for under-18s at www.dfes.gov.uk/consultations). From where I sit, the risks to this generation are two-fold – firstly, the obvious and most disturbing threats from exploitation of a very vulnerable age-group, and then the longer term effects of this dubious media content upon what will become the parents and government in the next 10-20 years. Who will be the White Knights when society's bad guys are getting their feet into even darker doorways of techno-access?

Keeping In Touch – And How!

As a "Times" reader every Saturday (the only issue I have time to read), I occasionally drag myself away from the despondency of the "Money" supplement and wander into softer territory with the "Body and Soul" section, reflecting those things that are beneficial and therapeutic for the, er, body and soul. On 8 September, B&S published some statistics on email practices and claimed that some people have been known to check their emails 40 times a minute!!

I sincerely hope that's what is colloquially known as a "mis-pront" because that means switching between applications and back once every second and a half – fast enough to replicate a slow strobe light!

And Finally …

Depending upon when this Journal gets published, delete as appropriate:

- On behalf of the IRMA Committee, may I wish you a Very Happy Christmas and Prosperous New Year.
- Gosh, hasn't it been hot?

(Well, it could be Christmas and still be hot – see the antipodes – Ed.)

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

e-Discovery Laws

The Australian Federal Court is expected to release a practice note in December 2007, to come into effect early in 2008, relating to e-discovery. The new rules are expected to emulate the United States 2006 Federal Rules of Civil Procedure which impose strict obligations on companies on their handling of electronically stored information and ensuring its availability for commercial litigation. The scope of electronic discovery includes information held on emails, instant messaging, voicemail and VOIP communications, files held on laptops, blackberries and other handheld devices and mobile phones, PowerPoint files, pdfs, and storage devices including USB drives and discs.

Discovery is the process by which parties in litigation request documents from each other prior to trial, relating to the facts in dispute.

The aim of the legislation is to bypass the adversarial nature of court cases over the nature and existence of information held electronically by requiring both parties to meet in a "pre-discovery conference" before any case comes to court and agree as to what records exist relating to the facts of the case in a non-adversarial manner, and ensure that these records are available to the court.

Most organizations already have policies and procedures in place in relation to hard copy documents and will have to emulate this in relation to electronic documents. In many cases new systems will have to be introduced to manage the storage, cataloguing and efficient retrieval of information from the many locations and formats where it may exist.

Additional legal risks will exist in the following areas:

- Organisations which are unable to retrieve information required by the courts
- Organisations which are required to retrieve information but are judged to have deleted that information intentionally to frustrate proceedings or through routine culling after the commencement of litigation.
- Organisations which have preserved information unnecessarily which is subsequently used against them in litigation.

Diary of a Busy Connector

Andrea Simmons

Below is a chronological review of meetings attended and initiatives undertaken, to give you a flavour of the level of activity with the BCS Security Forum. For information, the BCS itself is the 29th most mentioned organisation in the industry and receives on average 4 mentions a day in the press. Let's hope that level of impact continues to increase.

In a recent survey carried out by an industry colleague, the BCS came out as one of the top 6 networking forums. The question has been posed to me – "Is their any reason why the BCS forums (including IAAC) do not have a joint activity programme with ISSA, IISP, IISyG, ISACA and iBSIG (1-5 in the survey)." Given the level of interaction below – you can see that I am doing my best to provide an increased level of *connection*.

- On **29th August**, I met with Nigel Jones, new director of the Cyber Security KTN to begin the forging of a stronger relationship.

- On **3rd September**, I spoke at the Charity Commission IT Directors Group (CCitDG) AGM event in London.

- On **4th September**, BCS London hosted an IAAC workshop on Identity Assurance entitled *Examining the Needs and Concerns of the Citizen.*

- On **7th September**, I attended the last day of the CAMIS Conference. (*from the KTN newsletter)* – Dr Peter Trim ran an excellent conference over 3 days at Birkbeck University of London in early September. The core theme of the conference was 'Strategising resilience and reducing vulnerability'. As CAMIS stands for the Centre for Advanced Management and Interdisciplinary Studies, it was right that the programme ranged broadly, including aspects of emergency management, disaster recovery, international crises and corporate security. It was a useful reminder of how many of the problems we face are shared across many sectors, yet we have a tendency to find our own solutions in discreet and separate forums. Further information about CAMIS's interdisciplinary work is available from Peter Trim.) I gave a presentation on the complexity of the language we use and the placement of the multiplicity of organisations involved in the space, which often serves to cloud communication rather than enhance it. The result of this presentation has been two-fold:

  1) A request to write a chapter of a book for Peter Trim – currently on the title of the conference

  2) A request to lecture on the concept of Resilience and its origins for a new Cranfield MSc commencing January 2008

- I attended the BCS/ICS Joint 50th /40th Anniversary celebration dinner in Dublin on **20th September** at which Bob McLaughlin, Past BCS President (and current BCS Trustee) gave an hilarious, raucous and inappropriate after dinner speech, but I didn't tell you that ☺

- On **26th September**, BCS hosted a EURIM working party to discuss papers for MP Alun Michael for his presentations at Parliament and IT on 18th October and future discussion at the Internet Governance Forum planned Rio meetings. There will be significant follow-on from this, placing the BCS in a very influential position in the coming months.

- Discussions have taken place with EEMA to collaborate on the Birmingham Branch annual Security Conference potentially in **June/July 2008**. I attended a BCS Birmingham branch meeting to discuss this on **1st October**.

- A joint event between HIF, Ethics and Security Forum took place on **2nd Octobe**r on the issues of data management within the health sector in particular (disclosure, management, security and retention). Tom Parker and Phil Cracknell from the SFSP spoke extremely well and sparked lively afternoon discussion.

- Les Fraser, Roger Dean and Prof Brian Collins and I, amongst many others, all attended the IT Celebration dinner at the Guildhall on **3rd October**. A very pomp and pageant laden event (!) but incredibly well run. Food and wine in abundance and a great networking opportunity. Key learning point – the WCIT have just approved a Security Forum. Anyone with any contacts or info, please advise me ASAP.

- I attended Prof Fred Piper's networking dinner on **4th October** at RHUL, in the Picture Gallery. Austere surroundings, good food, great company and again, busy networking ☺

- On **8th October**, I attended a BCS Birmingham branch talk on Pornography, the Internet and the Law. Most enlightening and worrying in equal measure.

- BCS London hosted an EEMA workshop on Digital Signatures on **11th October** – this event was better attended than EEMA were hoping for and very lively debate ensued regarding the differences in the legalities across the various European states and how much this hampers interoperability etc.

- BCS London hosted another IAAC workshop on Identity Management – the Government's role and responsibilities – on **16th October**. Sir Edmund Burton the new chair was in attendance. There are some key recommendations that need to be presented to government and Sir Edmund is seeking the right path for IAAC to follow in delivering these.

- The 3rd Hot Topic Event hosted by the BCS Security Forum (and sponsored by Gartner) is now lined up

Diary of a Busy Connector

by ISDWG for **28th November** – in the subject area of IS Professionalism. Please email me if you wish to attend.

- A controversial conference is planned for **7th December** in conjunction with the Cyber Security KTN and the Trusted Computing Project – on the subject of *Enabling trusted access to e-services*. Again, please email me if you wish to attend.
- We are hosting the ISO 17799 User Group at BCS Southampton Street on **10th December** for their Annual Conference. The DTI has removed itself from their Secretariat support function and it is intended that the BCS take this over.
- Cyber Security KTN and Intellect (see below) have shared their respective work programmes for next year with a view to ensuring knowledge of forthcoming activities and opportunities for BCS Security Forum to be engaged. We will similarly share ours once done and then need to ensure cross fertilisation of respective Events Calendars.

Intellect 2007 Programme of activity

The agenda for 2008 was discussed at the last September Management Committee meeting. Please see below dates and topics agreed:

- ***Monday, 10 March 2008, 16:00 to 18:00 – "Contingency planning, home working and security"***

  Changing work practices and patterns due to broadband, transport, mobile working. Last minute contingency planning due to flooding, strikes, threats of flu viruses and the impact these will have on businesses especially from a security and privacy of their data and information point of view.

- ***Monday 12 May 2008, 16:00 to 18:00 – "Debate around Security and the future generation" This house believes....***

  A debate over the issue of social networking, the working practices of new generations, changes in business communication, the legal allowance on monitoring staff communication and how businesses could be losing vital information and staff depending on their view of security. Does the new generation pose a greater threat to business then ever before?

- ***Monday 7 July 2008, 16:00 to 18:00 – "Data Destruction and legal implications/requirements"***

  How do people destroy data, what works and what doesn't? What are the legal implications if you don't destroy data properly? Who could still access your data? What legislation must companies comply with? How do you protect your employees and Board?

Intellect welcome BCS contribution in their meetings. Please do let me know if you wish to attend any of the meetings.

Finally, for information, the 2006 ENISA "Who is Who Directory on Network and Information Security" has no mention of the BCS Security Forum. Let's hope that the next edition does!

Andrea is our Security Forum Manager representative.

Phone: 01905 356268
Mobile: 07961 508775

Email: andrea.simmons@bcs.org.uk
Web: www.bcs.org/security

Computer Forensics

John Mitchell

Introduction

'The moving finger writes and having writ moves on...' wrote Omar Khayyam some 900 years ago. What he did not foresee was the possibility of the text being composed on a device that could retain the imprint of the writing even after the paper on which it had been printed was destroyed. The role of forensic computing is very varied, but really falls into two main areas: criminal investigation and civil litigation.

Criminal cases usually require the retrieval of some information to support, or refute, a case being bought by the State. The most important part of any retrieved data item is usually the date and time it was created, the timestamp, as this usually ties in with some other evidence that is being presented. Proving the date and time is fraught with problems however, as we will discuss later. With the growth of the Internet, the problems associated with proving who originated something, from where and when, is becoming a major problem. With many international criminal organisations using the net for communication and data storage, the problem of decoding encrypted data is vexing the minds of the law enforcement bodies. This, coupled with the length of time that an investigation can take, often provides a warning to the perpetrators that allows them to move their activities to another part of the world and the whole investigative process may have to start again.

The *civil* cases usually revolve around contractual issues and requires the piecing together of what was intended and then comparing that with what has been provided. As the problem tends to be one of expectation it is not too surprising to find that the two sides have different views on what the deliverable should have been. The job of the investigator is firstly to decide what was reasonable and then to ascertain whether that marker has been met. This usually requires establishing the functionality of the system, its speed of response, the reliability of the documentation and the ongoing maintainability of the system. As the 'other side' will usually have their own expert there can be an interesting tussle in establishing the 'truth'. It never ceases to amaze me that the two sides can be well down the road of expensive litigation before they call in a couple of experts to advise them. It more often becomes a case of macho management, rather than sensible debate, with both sides hoping that 'their' expert can provide the coup de grace. In reality, the experts are there to guide the court and they usually reach agreement on what has happened and what should have been delivered long before their clients are ready to listen to reason.

The Evidence

Computer evidence exists on computer hard disk drives and other computer media at three different levels, two of which are not visible to the computer user. Such evidence is fragile and it can easily be destroyed through something as simple as the normal operation of the computer. Electromagnets and planted destructive Trojan horse programs are other hazards that can permanently destroy computer evidence in just a few moments.

Unlike paper evidence, computer evidence often exists in many different forms, with earlier 'draft' versions still retained on the same media as the final copy. Knowing the possibility of their existence means that alternate formats of the same data can be discovered. An expert identifying more evidence possibilities than originally requested can enhance the discovery process. In addition, during on-site premise inspections in cases where computers are not actually seized, the forensics expert can quickly identify places to look, signs to look for, and additional information sources for relevant evidence. These may take the form of earlier versions of data files that still exist on the computer's disk or on backup media, or differently formatted versions of data, either created or treated by other application programs (e.g. word processing, spreadsheet, e-mail, scheduling, or graphic).

Who Uses the Evidence?

Many types of criminal and civil proceedings make use of evidence revealed by computer forensics specialists:

- Criminal Prosecutors use computer evidence in cases where incriminating documents have been stored electronically;
- Civil litigators make use of personal and business records found on computer systems that bear on fraud, divorce, discrimination, and harassment cases;
- Insurance Companies may be able to mitigate costs by using discovered computer evidence of possible fraud in accident, arson, and compensation cases;
- Corporations hire computer forensics specialists to ascertain evidence relating to sexual harassment, embezzlement, theft or misappropriation of trade secrets and other internal/confidential information;
- Law enforcement officials frequently require assistance in pre-search warrant preparations and post-seizure handling of computer equipment;
- Individuals hire computer forensics specialists in support of possible claims of wrongful dismissal, sexual harassment, or age discrimination.

Securing the Evidence

Law enforcement officials normally seize computers during the execution of a search warrant. Depending on the circumstances and scope of the search warrant, all computer hardware, software and manuals should be taken for evaluation as potential evidence. Some prosecutors may view this as overly broad. However, the ability to process and examine the evidence may be directly tied to special hardware, software and/or written instructions contained in manuals. Because computer technology changes so quickly, it may be impossible to obtain similar or outdated hardware or instruction manuals from other sources. Printers, tape drives, optical drives, hardware manuals and software manuals, should all be taken. Pay particular attention to possible passwords that may have been written down near the computer. Encrypted files can cause serious difficulties and finding a password scrawled on a desk calendar may help make the case.

Many corporations and government

agencies are becoming involved with computer evidence relating to internal investigations and internal audits. Corporate computer specialists should follow the same procedures used in criminal investigations, because it is usually unknown if criminal proceedings will follow. Following accepted computer evidence processing procedures will ensure that the case meets the requirements for both civil and criminal trial purposes. In a corporate or government setting, the ability to seize a computer and evaluate its data will be governed by corporate policy and privacy laws. For this reason, it is essential that corporate legal counsel be consulted before taking any steps to seize or process a corporate computer. In the absence of a corporate policy covering computer evidence and privacy issues, corporate computer specialists could be exposing themselves and the corporation to litigation.

Caution should always be used in the shutdown and transport of the subject computer. To preserve the image on the screen, a photograph or camcorder image of the screen display may be appropriate. Then a decision has to be made as to whether or not the computer should be unplugged from the power supply, or shut down systematically based on the requirements of the operating system. Unfortunately, there is no correct answer and there are risks in taking either course of action. The decision will depend on the particular facts involved, the operating system involved, and judgement. On balance, I consider it safer to disconnect the computer from its power supply, whether it is stand alone, or networked. If the system is protected by an uninterruptible power supply disconnect the power to the machine from the machine side of the UPS to ensure an immediate break of power.

Care should be taken when using the keyboard to enter operating system commands. One press of a key may trigger destructive memory resident programs that have been planted on the computer.

If seizure of the computer is carried out when the system is attended, any individual attending the computer should be immediately removed from the vicinity. One press of a pre-arranged key combination can destroy all evidence stored on a hard disk. Consider using a subterfuge to remove the operator from the computer to eliminate the possibility of the destruction of potential evidence. Seizure planning is very important and this is especially true if the probability of destructive processes exist.

Evidence Gathering Concerns

The initial and primary job is to preserve the computer evidence and to transport the computer to a safe location where a complete bit stream backup can be made. You also want to ensure that the computer system can be reconfigured to match the configuration in which it was found. For this purpose, it is wise to take pictures of the complete computer system from all angles. Wires should be marked so that they can be correctly reconnected. Also, the computer should be clearly marked as evidence and stored out of reach of inquiring co-workers. Chain of evidence is as relevant when it comes to computers as any other form of evidence. Be sure to document the time, date and circumstances surrounding the actual seizure of the computer. Every effort must be made to show that no one could have made changes to the information contained on a seized computer system. Without such an assurance, countless hours of processing effort may be wasted and the case lost.

Another concern here relates both to storage devices and network servers, because if either of these are present then the data the investigator is looking for may be held on a device that is not being uplifted for imaging. Of particular interest is the Folder Redirection functionality in W2K/WinXP. If this has been activated then although the My Documents folder appears to the user as if it is held on their workstation the folder is actually physically located on a network server. The purpose behind this functionality is to enable the workstation to be replaced if / when required whilst minimizing disruption to the user. Great idea, but it does make life complicated for an investigator!

The computer investigator needs to be worried about destructive software planted by the computer owner. He also needs to be concerned about the operating system and applications. Evidence is easily found in typical storage areas, e.g., spreadsheet, database and word processing files, but evidence can also reside in slack space, erased files, the Windows swap file, email files and Internet temporary files. Such evidence is usually in the form of data fragments and it can be easily overwritten by something as simple as the booting of the computer and/or the running of the operating system. For example, when Windows starts, it creates new files and opens existing ones as a normal process. This situation can cause erased files to be overwritten and data previously stored in the Windows swap file to be altered or destroyed. Furthermore, Windows has a habit of updating directory entries for files as a normal operating process. These file dates are very important from an evidence standpoint. Another concern of the computer investigator, is the running of any programs on the subject computer. Criminals can easily modify the operating system to destroy evidence when standard operating systems commands are executed. Standard program names and familiar Windows program icons can also be altered and tied to destructive processes.

When it comes to computer evidence, paranoia is a good personality trait to have. Do not operate a suspect computer until a complete backup has been made of all storage devices. Standard computer backups won't do and a full bit stream backup is necessary. In the bizarre world of computer evidence, you should always assume that things will go wrong. Once computer evidence has been destroyed or altered, it is unlikely that it can ever be reconstructed.

Tools of the Trade

Computer forensic tools are basically computer software. Computer forensic specialists guarantee accuracy of evidence by using time tested evidence processing procedures and the use of multiple software tools developed by different developers. The use of different tools to validate results is important in order to avoid inaccuracies introduced by software design flaws and. It is a mistake for a computer forensics specialist to put all of his eggs in the same basket by using just one tool to preserve, identify, extract and validate the computer evidence. Cross validation through the use of multiple tools and techniques is standard in all the forensic disciplines. When this procedure is not used, it enables lawyers to challenge the efficacy of the software tool used and thus the integrity of the results.

Many inherent problems associated with computer evidence gathering disappear when tried and proven procedures are followed. The very first objective after securing the computer is to make a complete bit stream backup of all computer data before it is reviewed or processed. This should normally be done before the computer is operated. Preservation of evidence is the primary element of all criminal investigations and computer evidence is no exception. Evidence can reside at multiple levels and in strange locations. These levels include allocated files, slack space and erased files. It is not enough to do a standard backup of a hard disk drive. To do so would eliminate the slack and erased file space (see later). Without backing up evidence in these areas, the evidence is susceptible to damage and/or modification by the computer investigator. Bit stream backups are much more thorough than standard backups. They involve the copying of every bit of data on a storage device and usually two copies are made of the original. Any processing should be performed on only one of the backup copies. The original evidence should be preserved at all costs. After all, it is the 'best evidence' available.

Forensic Computing Rules

The computer forensics specialist will take into considerations the following areas when attempting to identify and retrieve evidence from a system computer system:

- Protect the suspect computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction;
- Discover all files on the subject system. This includes existing normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files;
- Recover all, or as much as possible, of discovered deleted files;
- Reveal, to the extent possible, the contents of hidden files as well as temporary, or swap files used by both the application programs and the operating system;
- Access, if possible and if legally appropriate, the contents of protected or encrypted files;
- Analyse all relevant data found in special and typically inaccessible areas of a disk. This includes unallocated space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as 'slack' space in a file (the remnant area at the end of a file, in the last assigned disk cluster, that is unused by current file data, but which may be a possible site for previously created and relevant evidence);
- Prepare an overall analysis of the subject computer system, as well as a listing of all possibly relevant files and discovered file data;
- Provide an opinion of the system layout, the file structures discovered, any discovered data and authorship information, any attempts to hide, delete, protect, encrypt information, and anything else that has been discovered and appears to be relevant to the overall computer system examination;
- Provide expert consultation and/or testimony, as required.

The main processes are expanded below.

Main Computer Forensic Processes

Shut Down the Computer

Depending upon the computer operating system, this usually involves pulling the plug or shutting down a network computer using relevant commands required by the network involved. Ideally, a digital camcorder can be used to record the shutdown process in real-time. Consideration should be given to possible destructive processes that may be operating in the background. These can be in memory, or available through a network, or connected modem. Depending on the operating system involved, a password protected screen saver may also kick in at any moment. This can complicate the shutdown of the computer. Generally, time is of the essence and the computer system should be shut down as quickly as possible.

Document the Hardware Configuration of the System

It is assumed that the computer system will be moved to a secure location where a proper chain of evidence can be maintained and evidence processing can begin. Before dismantling the computer, it is important that pictures are taken of the computer from all angles to document the system hardware components and how they are connected. Again, the use of a digital camcorder is ideal. Labelling each wire is also important so that it can easily be reconnected when the system configuration is restored to its original condition at a secure location.

Transport the Computer System to A Secure Location

This may seem basic but all too often seized computers are stored in less than secure locations. It is imperative that the suspect computer is treated as evidence and it should be stored out of reach of curious computer users. All too often, individuals operate seized computers without knowing that they are destroying potential evidence and the chain of evidence. Furthermore, a seized computer left unintended can easily be compromised. Evidence can be planted on it and crucial evidence can be destroyed. A lack of a proper chain of evidence can make inadmissible any evidence collected. Lacking a proper chain of evidence, how can it be argued that relevant evidence was not planted on the computer after the seizure?

Make Bit Stream Backups of Hard Disks and Other Media

The computer should not be operated and computer evidence should not be processed until bit stream backups have been made of all hard disk drives and other media. All evidence processing should be done on a restored copy of the bit stream backup rather than on the original computer. The original evidence should be left untouched unless compelling circumstances exist. Preservation of computer evidence is vitally important. It is fragile and it can easily be altered or destroyed. Often such alteration or destruction of data is irreversible. Bit stream backups are essential for any serious computer evidence processing.

Mathematically Authenticate Data on All Storage Devices

You want to be able to prove that you did not alter any of the evidence after the computer came into your possession. Such proof will help you rebut allegations that you changed or altered the original evidence. Forensic tools will calculate a check sum for the original data and append this to the bit stream copy for subsequent verification. Forensic software authenticates data using at least a 128-bit level of accuracy. Such a large key provides a good degree of certainty that the data has not been subsequently modified.

Identify File, Program and Storage Anomalies

Encrypted, compressed and graphic files store data in binary format. As a result, a text search program cannot identify text data stored in these file formats. Manual evaluation of these files is required and in the case of encrypted files, much work may be involved. Reviewing the partitioning on seized hard disk drives is also important. The potential exists for hidden partitions and/or partitions formatted with other than a DOS compatible operating system. When this situation exists it is comparable to finding a hidden hard disk drive and volumes of data and potential evidence can be involved. The partitioning can be checked with any number of utilities. When hidden partitions are found, they should be evaluated for evidence and their existence should be documented. It makes sense to evaluate the files contained in the Recycle Bin. The Recycle Bin is the repository of files selected for deletion by the computer user. The fact that they have been selected for deletion may have some relevance from an evidentiary standpoint. If relevant files are found, the issues involved should be documented.

Document the System Date and Time

The dates and times associated with computer files can be extremely important from an evidence standpoint. However, the accuracy of the dates and times is just as important. If the system clock is one hour slow because of daylight-saving time, then file time stamps will also reflect the wrong time. The operator may have set the date/time of the computer incorrectly to start with, or may have access to powerful utility programs that allow the subsequent alteration of the timestamp. The software itself may timestamp the transaction incorrectly and the computer's clock may have been altered several times to cloud the issue. To adjust for these inaccuracies, documenting the system date and time settings at the time the computer is taken into evidence is essential.

Depending on the forensic tools being used it may be necessary to boot the suspect computer under controlled conditions in order to obtain the internal date and time settings. This is usually achieved by booting the machine from media containing a controlled version of an operating system. It may be necessary to load the system configuration option to achieve this as some machines are configured not to boot from the floppy drive. The use of a camcorder to record the event is desirable as it could be held that changing the computer's configuration could have changed the data content. Hence the need to obtain a bit stream image before doing anything else.

Prepare a List of Key Search Words

Modern hard disk drives are so large that it is all but impossible for a computer specialist to manually view and evaluate every file on a computer's hard drive. Therefore, automated forensic text search tools are needed to help find the relevant evidence. Usually, some information is known about the allegations, the computer user and the alleged associates that may be involved. Gathering information from individuals familiar with the case to help compile a list of relevant key words is important. Keeping the list as short as possible is important and common words or words that make up part of other words should be avoided.

Examine the Windows Swap File

The Windows swap file is potentially a valuable source of evidence and leads. In the past this tedious task was done with hex editors and the process took days. By using automated tools, that process now takes just a few minutes. Where Windows 95 upward is involved, the swap file may be set to be dynamically created as the computer is operated. This is the default setting and when the computer is turned off, the swap file is erased. However, not all is lost because the content of the swap file can easily be captured and evaluated in much the same way as any other erased file can be recovered.

Evaluate File Slack

File slack is a data storage area of which most computer users are unaware. It consists of raw memory dumps that occur during the work session as files are closed. The data dumped from memory ends up being stored at the end of allocated files, beyond the reach or the view of the computer user. Specialised forensic tools are required to view and evaluate file slack and it can provide a wealth of information and investigative leads. Like the Windows swap file, this source of data can help provide relevant key words and leads that may have previously been unknown. Such keywords should be added to the computer investigator's list of key words for use later. Because of the nature of file slack, specialised and automated forensic tools are required for evaluation.

Evaluate Erased Files

Operating system delete functions do not completely erase file names or file content. Many computer users are unaware the storage space associated with such files merely becomes unallocated and available to be overwritten with new files. Unallocated space is a source of significant 'security leakage' and it potentially contains erased files and file slack associated with the erased files. Often the operating system's undelete program can be used to restore the previously erased files. Like the Windows swap file and file slack, this source of data can help provide relevant key words and leads that may have previously been unknown to the computer investigator. Because of the nature of data contained in unallocated space and its volume, specialised and automated forensic tools are required for evaluation.

Identify Email Storage Areas

If the computer has been used for email, then it is likely that relevant correspondence will be held in the email folders.

Identify Internet Storage Areas

If the computer has been used for accessing the Internet, then it is likely that a wealth of information will be held in Internet folders, favourites and temporary Internet files. The ‘cookie’ repository should not be overlooked, as information here will reveal some of the sites visited.

Search All Areas for Key Words

The list of relevant key words identified in the previous steps should be used to search all relevant computer hard disk drives and other media. There are several forensic text search utilities available in the marketplace. It is important to review the output of the text search utility and equally important to document relevant findings. When relevant evidence is identified, the fact should be noted and the identified data should be completely reviewed for additional key words. When new key words are identified, they should be added to the list and a new search should be conducted.

Steganographic Awareness

Steganography is the process by which data can be hidden in images. A key protects the data so hidden and a casual browse of the image will show nothing amiss. Indeed, the only sign that steganography is being is used may be the existence of a steganographic application on the disk. The investigator needs to be aware of the names of these programs, but also aware that they are easily renamed to something innocuous. In some cases the only indication that a program is of the steganographic school comes when it is run.

Document File Names, Dates and Times

From an evidence standpoint, file names, creation dates, last modified dates and times can be relevant. Therefore, it is important to catalogue all allocated and 'erased' files.

Document the Findings

As indicated in the preceding steps, it is important to document your findings as issues are identified and as evidence is found. Documenting all of the software used in your forensic evaluation of the evidence, including the version numbers of the programs used, is also important.

Retain Copies of Software Used

As part of your documentation process, ensure that a copy of the software used is included with the output of the forensic tool involved. Normally this is done on an external storage device. When this documentation methodology is followed, it eliminates confusion as to which version of the software was used to create the output. Often it is necessary to duplicate forensic processing results during or before trial. Duplication of results can be difficult or impossible to achieve if the software has been upgraded and the original version used was not retained. There is a high probability that you will encounter this problem because most commercial software is upgraded routinely but it may take years for a case to go to trial.

Only Use Licensed Forensic Software!

Be sure that you are legally licensed to use the forensic software. Software pirates do not stand up well under the rigours of a trial. Lawyers may question software licensing and you do not want to testify that you used unlicensed software in the processing of computer evidence, as software piracy is a criminal violation of copyright laws. Where appropriate, mention in your documentation that the forensic software used was licensed

Conclusions

The preservation of computer evidence is the most important element of computer evidence processing. However, the proper documentation of the steps taken during the evidence processing also ranks as a top priority. Good documentation tied to sound processing procedures is essential for success. Without the ability to reconstruct accurately what has been done, crucial evidence may be subject to question. More importantly, the qualifications of the expert witness can become an issue if the computer evidence processing was done haphazardly. Shortcuts should be avoided at all costs.

One of the main problems associated with criminal cases is that the burden of proof is so great that extensive investigation is required. A further problem is that with the increasing use of personal computers, everyone tends to consider themselves experts in computing. It is important that the forensic investigator can present a case in a way that will not antagonise a jury, but which at the same time eliminates the likelihood of misinterpretation, due to misguided knowledge.

Forensic computing, whether of a criminal, or civil nature, requires attention to detail, a methodical approach and good record keeping. It brings together many skills: computing; auditing; the law, interviewing, report writing, but above all, patience. This last skill is the most difficult to learn, as it is easier to destroy evidence by switching on a suspect computer without realising that the very act of switching it on may contaminate the evidence, than it is to retrieve it by careful thought and thorough analysis.

The evidence is one thing, interpretation is another. Two experts will often agree on the accuracy of the evidence, but will disagree on its interpretation. Now that is where the fun really starts!

John Mitchell is Managing Director of LHS Business Control

47 Grangewood, Potters Bar,
Hertfordshire, EN6 1SL, England

Tel: +44 (0)1707 851454
Fax: +44 (0)1707 851455
Cell: +44 (0)7774 145638

Email: john@lhscontrol.com
Internet: www.lhscontrol.com

HUMOUR PAGES

Wisdom?

You never really learn much from hearing yourself talk. *George Clooney*

The trouble with beauty is that it's like being born rich and getting poorer. *Joan Collins*

Both optimists and pessimists contribute to our society. The optimist invents the plane and the pessimist the parachute

Plane travel is nature's way of making you look like your passport photo.

The formula for successful relationship is simple: treat all disasters as if they were trivialities, but never treat triviality as if it were a disaster. *Quentin Crisp*

Money can't buy you happiness, but it can buy you a yacht big enough to pull up alongside it. *David Lee Roth*

They say marriages are made in heaven but so are thunder and lightning. *Clint Eastwood*

The most important thing a father can do for his children is to love their mother. *Theodore Hesburgh*

It's just like magic, when you live by yourself all your annoying habits are gone. *Merrill Markoe*

For fast-acting relief, try slowing down. *Lily Tomlin*

Those who do not know how to weep with their whole heart don't know how to laugh, either. *Golda Meir*

"Those who are too smart to engage in politics are punished by being governed by those who are dumber" – *PLATO*

Factoids

The shortest war in history was between Zanzibar and England in 1896. Zanzibar surrendered after 38 minutes.

Vatican City is the smallest country in the world, with a population of 1,000 and a size 108.7 acres.

The youngest pope was 11 years old.

The San Francisco Cable cars are the only mobile National Monuments.

If a statue in the park of a person on a horse has both front legs in the air, the person died in battle; if the horse has one front leg in the air, the person died as a result of wounds received in battle; if the horse has all four legs on the ground, the person died of natural causes.

The Pentagon, in Arlington, Virginia, has twice as many bathrooms as is necessary. When it was built in the 1940s, the state of Virginia still had segregation laws requiring seperate toilet facilities for blacks and whites.

The Eisenhower interstate system requires that one mile in every five must be straight. These straight sections are usable as airstrips in times of war or other emergencies.

The highest point in Pennslyvania is lower than the lowest point in Colorado.

State with the highest percentage of people who walk to work: Alaska.

Maine is the only state whose name is just one syllable.

In Minnesota, it is illegal to cross state lines with a duck on your head.

In Indiana, it is illegal to ride public transportation for at least 30 minutes after eating garlic.

When the University of Nebraska Cornhuskers play football at home, the stadium becomes the state's third largest city.

Hang On Sloopy is the official rock song of Ohio.

Dueling is legal in Paraguay as long as both parties are registered blood donors.

In England, the Speaker of the House is not allowed to speak.

Winston Churchill was born in a ladies' room during a dance.

The cruise liner, Queen Elizabeth II moves only six inches for each gallon of diesel that it burns.

China has more English speakers than the United States.

If the population of China walked past you in single file, the line would never end because of the rate of reproduction.

The world's youngest parents were 8 and 9 and lived in China in 1910.

City with the most Rolls Royce's per capita: Hong Kong.

The national anthem of Greece has 158 verses. No one in Greece has memorized all 158 verses.

Saudi Arabia imports sand from Scotland and camels from North Africa.

Average number of days a West German goes without washing his underwear: 7

Percentage of Africa that is wilderness: 28%
Percentage of North America that is wilderness: 38%

Percentage of American men who say they would marry the same woman if they had it to do all over again: 80%
Percentage of American women who say they'd marry the same man: 50%

35% of the people who use personal ads for dating are already married.

You share your birthday with at least 9 million other people in the world.

February 1855 was the only month in recorded history not to have a full moon.

The winter of 1932 was so cold that Niagara Falls froze completely solid.

Saturn's density is so low that if it fell into a vast area of water, it would float

In Ancient Egypt, priests plucked every hair from their bodies, including their eyebrows.

Lovers in Elizabethan times would exchange "Love Apples" when plighting their troth. Peeled apples were kept under the respective armpits until saturated with sweat and then inhaled by male and female as a reminder of their love.

William Tell couldn't have shot an apple from his son's head with a crossbow because crossbows were unknown in Switzerland in the 13th century.

Americans eat 18 acres of pizza every day.

Between 1937 and 1945 Heinz produced a version of Alphabetic Spaghetti especially for the German market that consisted solely of little pasta swastikas.

Iceland consumes more Coca-Cola per capita than any other nation.

Coca cola was originally green.

Hershey's Kisses are called that because the machine that makes them looks like it's kissing the conveyor belt. (Hershey Squirts rejected for obvious reasons)

The cigarette lighter was invented before the match.

More than 50% of the people in the world have never made or received a telephone call.

23% of all photocopier faults worldwide are caused by people sitting on them and photocopying their buttocks.

In most advertisements, including newspapers, the time displayed on a watch is 10:10.

All of the clocks in the movie Pulp Fiction are stuck on 4:20.

111,111,111 x 111,111,111 = 12,345,678,987,654,321

Banging your head against a wall uses 150 calories an hour. (See, your TIMe could have been put to better use than reading all of this senseless information)

Intelligent people have more zinc and copper in their hair. (If you read this far, don't worry, they aren't talking about you)

C.V. Humour

Sunil Duggal, MD at Just IT Recruitment, receives hundreds of CVs and cover letters every day, some brilliant and others appalling. In a bid to educate job seekers, he identifies the 'don't dos' by revealing some of the worst to land on his desk from potential candidates.

Here are the some of the best of the worst:

- The neurotic: a candidate submitted a password protected CV which could not be accessed;
- The evangelist: a candidate ended a covering letter with 'Jesus loves you';
- The banker: a candidate put their bank details on their CV;
- The cyber-criminal: a candidate put that their life's ambition was to be a hacker;
- The punctual one: a candidate put 'I'm good at timekeeping. I wake up at 6am on Monday, Wednesday and Friday' on their cover letter;
- The bone idle: a candidate sent across a generic template leaving gaps where there should have been information describing the job position they were applying for, and the company they were applying to;
- The enigma: a CV was submitted with no name or contact details;
- The pervert: CVs with inappropriate email addresses such as 'caught ****ing@school.com';
- The narcissist: a cover letter from a candidate with one objective – 'to please and attain supreme perfection';
- The adult film star: a CV was submitted including a photo more suitable for a glamour shoot.

Thoughts

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

If you must choose between two evils, pick the one you've never tried before.

Change is inevitable – except from vending machines.

Plan to be spontaneous........ tomorrow.

Hard work pays off in the future. Laziness pays off now!!

Why do we put garments in a suitcase, and suits in a garment bag?

If man evolved from monkeys and apes, why do we still have monkeys and apes?

If you throw a cat out a car window does it become kitty litter?

What has four legs and an arm? A happy pit bull.

I started to change my shirt, but then I changed my mind instead.

Do you ever stop to think and then forget to start again?

A conclusion is simply the place where you got tired of thinking.

What is a "free" gift? Aren't all gifts free?

Ninety-nine percent of lawyers give the rest a bad name.

"24 hours in a day... 24 beers in a case... coincidence?" Clyde asked.

Clyde's Law: You can't fall off the floor.

Eagles may soar, but weasels aren't sucked into jet engines.

If at first you don't succeed, skydiving is not for you.

For Sale: Parachute. Only used once, never opened, small stain.

Experience is something you don't get until just AFTER you need it.

Having a Smoking Section in a restaurant is a little like having a peeing section in a pool!

To succeed in politics, it is often necessary to rise above your principles.

A clear conscience is usually the sign of a bad memory.

If pro is the opposite of con, then what is the opposite of progress?

A diplomat is someone who can tell you to go to hell and make you feel happy to be on your way there.

Vital papers will demonstrate their vitality by moving from where you left them to where you can't find them.

The average woman would rather have beauty than brains, because the average man can see better than he can think.

Paranoids are people too. They have their own problems. It's easy to criticize, but if everybody hated you, you'd be paranoid, too.

Borrow money from pessimists – they don't expect it back.

Money can't buy happiness. But it sure makes misery easier to live with.

Money can't buy love. But it CAN rent a very close approximation.

To steal ideas from one person is plagiarism; to steal from many is research.

Everyone has a photographic memory. Some just don't have film.

If you are given an open-book exam, you will forget your book. COROLLARY: If you are given a take-home test, you will forget where you live.

The two most common elements in the universe are hydrogen and stupidity.

Nothing in the known universe travels faster than a bad check.

Clothes make the man. Naked people have little or no influence on society.

The trouble with doing something right the first time is that nobody appreciates how difficult it was.

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

If at first you don't succeed, destroy all evidence that you tried.

Two wrongs are only the beginning.

The sooner you fall behind, the more time you'll have to catch up.

It may be that your sole purpose in life is simply to serve as a warning to others.

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

Always remember to pillage BEFORE you burn. "Have fun storming the castle!!"

Deja Moo: The feeling that you've heard this bull before.

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

Paradoxes & Oxymorons....

1. Is it good if a vacuum really sucks?
2. Why is the third hand on the watch called the second hand?
3. If a word is misspelled in the dictionary, how would we ever know?
4. If Webster wrote the first dictionary, where did he find the words?
5. Why do we say something is out of whack? What is a whack?
6. Why do "slow down" and "slow up" mean the same thing?
7. Why do "fat chance" and "slim chance" mean the same thing?
8. Why do "tug" boats push their barges?
9. Why do we sing "Take me out to the ball game" when we are already there?
10. Why are they called "stands" when they are made for sitting?
11. Why is it called "after dark" when it really is "after light"?
12. Doesn't "expecting the unexpected" make the unexpected expected?
13. Why are a "wise man" and a "wise guy" opposites?
14. Why do "overlook" and "oversee" mean opposite things?
15. Why is "phonics" not spelled the way it sounds?
16. If work is so terrific, why do they have to pay you to do it?
17. If all the world is a stage, where is the audience sitting?
18. If love is blind, why is lingerie so popular?
19. If you are cross-eyed and have dyslexia, can you read all right?
20. Why is bra singular and panties plural?
21. Why do you press harder on the buttons of a remote control when you know the batteries are dead?
22. Why do we put suits in garment bags and garments in a suitcase?
23. How come abbreviated is such a long word?
24. Why do we wash bath towels? Aren't we clean when we use them?
25. Why doesn't glue stick to the inside of the bottle?
26. Why do they call it a TV set when you only have one?
27. Christmas oxymoron: What other time of the year do you sit in front of a dead tree and eat candy out of your socks?
28. Why are they called apartments when they are all stuck together?

Circular Reasoning

It was already late fall and the Indians on a remote reservation in South Dakota asked their new chief if the coming winter was going to be cold or mild. Since he was a chief in a modern society he had never been taught the old secrets. When he looked at the sky he couldn't tell what the winter was going to be like.

Nevertheless, to be on the safe side, he told his tribe that the winter was indeed going to be cold and that the members of the village should collect firewood to be prepared.

But being a practical leader, after several days he got an idea. He went to the phone booth, called the national weather service and asked, "Is the coming winter going to be cold?"

"it looks like this winter is going to be quite cold," the meteorologist at the weather service responded.

So the chief went back to his people and told them to collect even more firewood in order to be prepared.

A week later he called the national weather service again. "Does it still look like it is going to be a very cold winter?"

"Yes," the man at national weather service again replied, "It's going to be a very cold winter."

The chief again went back to his people and ordered them to collect every scrap of firewood they could find.

Two weeks later the chief called the national weather service again. "Are you absolutely sure that the winter is going to be very cold?"

"Absolutely," the man replied. "It's looking more and more like it is going to be one of the coldest winters we've ever seen."

"How can you be so sure?" the chief asked.

The weatherman replied, "The Indians are collecting firewood like crazy".

Management Committee

CHAIRMAN	Ross Palmer	chair.irma@bcs.org.uk
SECRETARY	Siobhan Tracey	Siobhan.Tracey@dsgiplc.com
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Adam Carden	adam.carden@scottish-southern.co.uk
JOURNAL EDITOR	John Mitchell	john@lhscontrol.com
WEBMASTER	Allan Boardman	allan@internetworking4u.co.uk
EVENTS PROGRAMME CONSULTANT	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON – IIA & NHS	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON – ISACA	John Mitchell	john@lhscontrol.com
MARKETING	Vacant	
ACADEMIC RELATIONS	George Allan	george.allan@port.ac.uk

SUPPORT SERVICES

ADMINISTRATION	Janet Cardell-Williams t: 01707 852384 f: 01707 646275	admin@bcs-irma.org

OR VISIT OUR WEBSITE AT	**www.bcs-irma.org**
	Userid = irmamembers
	Password = 4members07
		Members' area

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)

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

INDIVIDUAL MEMBERSHIP *(Includes BCS Affiliate membership)* £35
For details of BCS membership visit www.bcs.org

INDIVIDUAL MEMBERSHIP *(A member of the BCS)* FREE
BCS membership number: ___________________________

STUDENT MEMBERSHIP – Full-time only and must be supported by a letter from the educational establishment. *(An annual quota is in operation, so IRMA retains the right to close this level of membership at any time).* FREE
Educational Establishment: ___________________________

Please circle the appropriate subscription amount and complete the details below.
All communications from the Group are likely to be electronic.
Please tick this box to indicate you agree to be contacted this way. □

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE:
(STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY: (Please circle)
1 = Internal Audit
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
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

BCS IRMA SPECIALIST GROUP ADVERTISING RATES

Reach the top professionals in the field of Information Risk Management and Audit by advertising in the BCS IRMA SG Journal. Our advertising policy allows advertising for any security and control related products, service or jobs.

For more information, contact John Mitchell on 01707 851454, fax 01707 851455 email john@lhscontrol.com.

There are three ways of advertising with the BCS IRMA Specialist Group:

The Journal is the Group's award winning quarterly magazine with a very defined target audience of 350 information systems audit, risk management and security professionals.

Display Advertisements Rates:

- Inside Front Cover £400
- Inside Back Cover £400
- Full Page £350 (£375 for right facing page)
- Half page £200 (£225 for right facing page)
- Quarter Page £125 (£150 for right facing page)
- Layout & artwork charged @ £30 per hour

Direct e-mailing

We can undertake direct e-mailing to our members on your behalf at any time outside our normal distribution timetable as a 'special mailing'. Items for distribution MUST be received at the office at least 5 WORKING DAYS before the distribution is required. Prices are based upon an access charge to our members of £350.

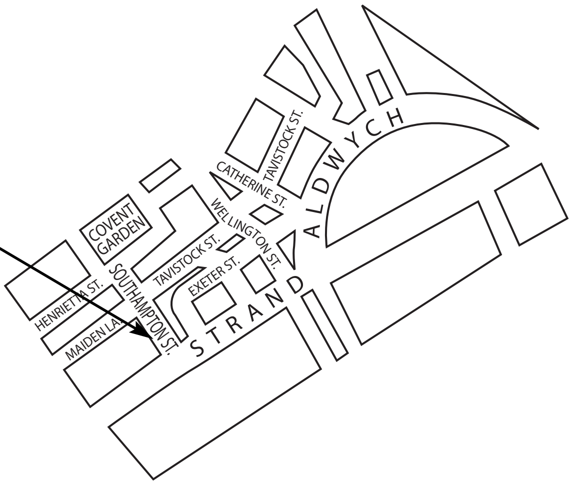
Contact

Administration

Janet Cardell-Williams,
49 Grangewood, Potters Bar, Hertfordshire EN6 1SL
Email: admin@bcs-irma.org
Website : www.bcs-irma.org

Meeting Venue unless otherwise stated

BCS, The Davidson Building,
5 Southampton Street,
London WC2 7HA


COVENT GARDEN
HENRIETTA ST.
MAIDEN LA.
SOUTHAMPTON ST.
TAVISTOCK ST.
EXETER ST.
WELLINGTON ST.
CATHERINE ST.
TAVISTOCK ST.
ALDWYCH
STRAND