IRMA
Information Risk Management & Audit
◆ A specialist Group of the BCS ◆

JOURNAL
Volume 18 Number 2 Summer 2008 ISSN 1741-4229

BCS
THE BRITISH COMPUTER SOCIETY

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
1 Apr	Radio-frequency identification (RFID)	Ken Munro	17.30	BCS London Office
27 May	AGM + Digital Forensics	Keith Foggon	17.00	BCS London Office
1 July	Payment Card Industry (PCI) Data Security Standard (DSS)	Simon Langley	17:30	BCS London Office
29 Sept	TBA	TBA	17.30	BCS London Office
15 Dec	TBA	TBA	17.30	BCS London Office
6 Jan 2009	TBA	TBA	17.30	BCS London Office
3 Feb 2009	TBA	TBA	17.30	BCS London Office
3 Mar 2009	TBA	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

Technical Briefings		Front Cover
Editorial	John Mitchell	3
Chairman's Corner	Ross Palmer	4
BCS IRMA SG AGM Report		5
Information Technology Legislative Update	Dr A.Abimbola	8
The Down Under Column	Bob Ashton	10
Members' Benefits Discounts	Mark Smith	11
Humour Pages		12
BCS Affiliated Membership Application		13
Management Committee		15
Advertising in the Journal		16
IRMA Venue Map		16

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 **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

What goes around comes around. When I announced last year that I would be hanging up my editorial pen I pledged to find a successor before doing so. Since its inception in the last century (late nineteen eighties) the Journal has had only three editors: Ginny Bryant, Rob Melville and myself. Finding another to take the Journal into its second decade was not easy, but lady luck stepped in and Rob Melville, who is now Director of MSc in Management at Cass Business School, has volunteered to again take on the role in conjunction with Mike Lavine of the John Hopkins University in the USA. This is exceptionally good news and I could not have asked for a better team to take the Journal forward.. I wish them every success and I look forward to being on the reading end of the next edition.

The government again faced condemnation after it emerged that 600 staff at Her Majesty's Revenue & Customs (HMRC) have been disciplined for misuse of personal data. The revelation that 192 staff had been disciplined last year, 180 in 2006 and 238 in 2005. was coupled with a report that HMRC has also discussed 11 data security incidents involving customer information with the Information Commissioner's Office since April 2005. No information was provided on the type of disciplinary action that was taken. If we assume that this is the proverbial tip of the iceberg, where only fifteen percent is visible above sea level, then we can extrapolate that perhaps 4,000 staff are regularly misusing our data without being caught. This is about five percent of HMRC's staffing. Taking this dodgy extrapolation further we can guestimate that when the proposed NHS central patients database goes live up to 15,000 of the 390,000 anticipated users will be using our data illegally. Going even further, if the Government gets its universal identity database, then perhaps one and a half million users may be accessing our data for nefarious purposes. The one good thing to consider is that as the data is likely to be woefully incorrect , then any conclusions they draw are likely to be incorrect too. 'Want some dodgy data mate? I've got the full identity database on these DVDs'. 'No thanks mate. If I want accurate data I'll use the Tesco database'.

The government is also pushing for the retention of all electronic communications for at least twelve months to help in its fight against terrorism and organised crime. How out of date can they be? The big boys either use couriers or meet in virtual worlds such as Second Life where their avatars do not look like them at all. 'What have you been doing today John?'. 'I've been tracking this Bin Laden lookalike in Second Life'. 'The one with the green beard?'. 'Yep, that's the one'. 'Idiot! That's me in deep cover'. The Information Commissioner says that we are sleep walking into a surveillance society where each one of us is currently caught on camera some three hundred times a day. Link this with the misuse of the RIPA legislation which is enabling councils (our obedient civil servants) to snoop on people who leave their bin lids open and it is apparent that we are not sleep walking into this surveillance society, but are being dragged into it by our elected representatives. The London congestion charge was meant to reduce traffic in the capital, but the cameras are routinely used by the police to track individual vehicles. The law of unintended consequences marches on with the Transport for London Oyster card, which is meant to make public transport cheaper and more convenient to use, but also enables an individual card, and by default its registered owner, to be tracked across London.

Recent TV adverts urging people to pay for their TV licences conclude with the words 'its all in the database'. If only they could ensure that it will remain there. If the government are serious about protecting our personal data they would separate key items over several separate databases so that a single hacker would only be able to retrieve part of the information: a name, but not the address; a sort code, but not the account number; a gender, but not the age; etc. Each database would have its own security and logging mechanisms which would be policed by suitable expert systems on a continuous monitoring basis. It would be expensive and require excellent development skills, but it is the only way to safeguard our data from unauthorised access and disclosure.

In this edition you will find a useful article on legal updates from Dr A Abimbola, a farewell column from our outgoing chairman Ross Palmer, a financial statement from Jean Morgan our treasurer, a down-under column from Bob Ashton and the usual list of member benefits from Mark Smith who has also sadly resigned from the Management Committee. You will notice from the financial statement that we have notional reserves of over £23,000. The reason that these are notional is that they have been sequested by the Society into its central reserves. Under the new accounting rules we no longer have access to these carefully husbanded resources, but I consider it essential that we account on a going concern basis, even if the Society has removed any incentive for us to do so.

Finally, to paraphrase John F Kennedy, a previous president of the USA, 'the torch has been handed to a new generation'. May its flame burn brightly into the future.

Chairman's Corner

Ross Palmer

What's in a name?

Hello again, IRMA Members!

Anybody got previous Phorm?

Quite a few puns have arisen recently using the name "Phorm" in various situations, like the corny title I have used above.

As an anagram phanatic (oops), I prefer to think of "Phorm" as a re-arrangement of the letters in the name of the little chap from "Vision On" many years ago and much as I would love to extol his virtues for the rest of this article, I really need to cut this drivel and get down to the serious bit.

As many of you will surely have heard, Phorm is a new online advertising company that uses behavioural profiling on behalf of its clients to analyse customer preferences – much along the lines of your Nectar or Tesco Clubcards, while you are gaining loyalty points in your local supermarket.

A few Internet Service Providers (ISPs) have contracted with Phorm to use its analysis products on their sites but with two varying conditions – "opt-out" and "opt-in". ISP customers do one or the other by default but can voluntarily opt for the alternative.

Extending the loyalty cards parallel, this is tantamount to putting an "X" in the box on the application phorm (sorry) NOT to receive marketing information when the next one in the same blurb may say to put an "X" in the box if you DO want to receive stuff "from our partners" … blah, blah. It can be most confusing but it is a quick personal decision that, if taken wrongly, can potentially enhance the coverage of your Inbox or doormat with junk mail!

Invasion of privacy is a very contentious issue here as is responsibility for it. BT, as an ISP, for example, uses "opt-out" (i.e. users positively need to DO something to avoid the marketing stuff heading their way) and any breach of the Data Protection Act will fall upon the ISP, who is technically the data controller.

ISPs, therefore, need to check the effects on their liability and, perhaps more importantly, their reputations, but it is commendable that Phorm is engaging in constructive public debate over the issue.

The "i" of the storm!

New inventions invariably result in teething problems and unexpected development directions. For example, when Percy Shaw was driving in thick fog and he saw his headlights reflected in the eyes of a cat walking towards him, he promptly invented the cat's eye, while legend has it that if the cat had been walking away from him, he would have invented the pencil sharpener.

Be that as it may, BBC's new iPlayer, developed for the benefit of on-line viewers who have missed a critical TV programme, has run into a spot of unexpected bother with the ISPs (those same eminent organisations mentioned in the previous section).

So successful has iPlayer become (even I use it!) that it is giving ISPs a headache over increased bandwidth use. The ISPs claim that the tab for upgrading networks should be borne by The Beeb, who, in return, believes the costs should be carried by ISPs.

I recently entered into an ISP contract for unlimited internet downloads, paying a hefty premium for the privilege, plus I am a TV Licence payer, so I know whose views I support.

Nevertheless, it should be an interesting outcome, if only to see whether it becomes resolved before the advent of CERN's particle-physics based "grid" (ostensibly providing speeds around 10,000 times faster than a typical broadband connection).

The Italian Job

Here was I, about to commit my Journal copy to Dr John, when what should I spot on today's BBC News website? "Italy posts income details on web".

Apparently, by error or design, the outgoing Italian government has published every Italian's declared earnings and tax contributions on the internet.

Well, that should give HMRC (they of the 2-disc special) a welcome opportunity to be smug … if only in relative terms.

"Thank you and goodnight"

If you have enjoyed reading this Journal column half as much as I have enjoyed writing it, then … well … I have enjoyed it twice as much as you, I guess.

However, this will be my last "Chairman's Corner" Journal contribution as I have decided to stand down from the IRMA management committee at the AGM in May, having served on it for five years with two as Chairman.

It's been really great meeting many of you at the monthly IRMA evening sessions in London and I hope to continue to do so but henceforth in the capacity of "one of the punters", so to speak.

I'd also like to pay a warm tribute to my colleagues on the committee, who are all card-carrying members of the "work hard – play hard" ethic and without whom none of the continual stream of very cheap (inexpensive, that is) professional education events could take place.

Thank you, guys 'n' gals, for being such a great team.

I now look forward to attending many more IRMA events but without causing my arms to morph (there you go – the answer to above!) into those of an orang-utan, due to carrying two fully-loaded wine bags from Basingstoke to London for each event in order to keep the catering costs down.

My first task will be to buy myself a guitar with a 25% longer-scale fret board …

Ross

IRMA Chair

BRITISH COMPUTER SOCIETY
INFORMATION RISK MANAGEMENT & ASSURANCE SPECIALIST GROUP

Minutes of Annual General Meeting

Held on Tuesday 27th May 2008 at BCS London Offices at 5 Southampton Street, London, WC2E 7HA

1. Apologies Received

- John Mitchell
- Allan Boardman

2. Approval of the minutes of the AGM held on the 2nd May 2007.

The minutes of the AGM held on the 2nd May 2007 were approved by the meeting.

Proposed by: Mark Smith
Seconded by: Jean Morgan

3. Chairman's report.

Ross Palmer presented his Chairman's Report for 2007/2008, which will be his final as he has decided to step down from the BCS IRMA committee in order to pursue other personal and professional interests.

BCS Organisational Changes

The past year has seen several changes that affect BCS IRMA and its membership and these are continuing as I speak. These have all involved the parent British Computer Society in its drive for increased professionalism.

Firstly, from 1 May 2008, all Specialist Group members have to be members of the BCS as a pre-requisite.

For the 2008/09 year, a free offer of a year's membership at whatever BCS level is appropriate for the member has been granted to all SG applicants and IRMA now no longer levies any fees.

This has pushed the IRMA membership up substantially but the subsequent effect on overall SG memberships in May 2009, when fees begin in earnest, can only remain to be seen, so watch this space.

As with other SGs, BCS has centralised the IRMA budget. This means that the substantial reserves built up by previous IRMA and forerunner CASG committees over the years have been absorbed into a central BCS pot from which IRMA can apply for funds – as can other SGs with fewer of their own reserves.

This has not so far caused IRMA financial problems, just a limited freedom as to how we request and use our funds and the need for more focused budgetary liaison with BCS.

BCS is also taking over the hosting of the IRMA website and membership database, which has caused some initial problems with database version control. Thus, if you have been mailed twice or not at all about events, etc., please accept our apologies.

Finally, the IRMA constitution is also changing in accordance with revised BCS wording for all SGs and this may be a material issue for the composition of IRMA's committee. For example, it will require the Chair, Secretary, Membership Secretary and Treasurer positions to be professional or chartered BCS members, which could restrict the availability of committee candidates.

Presentations

Despite difficulties in predicting exactly how many people will be attending sessions, IRMA has had another very successful year, hosting 8 evening presentations and one full day event in partnership with ISACA.

The diversity of topics has ranged between a number of topics, including "Risk Based Auditing", "Mobile and Network Security", "Inside the Minds of Convicted Fraudsters" and "Radio Frequency Identification" and including eminent and invigorating speakers such as Ian Kennedy, of Kent Police Digital Forensics Unit, Stan Dormer, of Mindgrove, and Ken Munro of Securetest.

A very successful full day event on the theme of Computer Crime was co-presented with ISACA in October, for which ISACA generously donated its share of the income to IRMA.

Also, committee members John Mitchell and Ross Palmer made external presentations respectively to the Advanced Programming Group and BCS Dorset.

The Committee

Sadly, November saw the death of our old IRMA friend Willie List, who was Chairman of this Specialist Group from 1981 to 1988 and who had been lined up for an evening session in this year's programme. John Mitchell published a warm tribute to his old committee friend and colleague in the Journal.

Speaking of tributes, I should like to give my heartfelt thanks for the immense support of the present IRMA management committee.

However, I regret to inform you that four long-serving members are also standing down as from this evening.

Firstly, Mark Smith, who has been mainly responsible for finding our speakers, often at very short notice, and for negotiating member deals. His links to Italy seem to have given him the persuasion skills of Don Corleone.

Siobhan Tracey, our Secretary and fairly vociferous team member, has organised and presented a number of our sessions and always kept the AGM protocols on track.

Allan Boardman, the IRMA webmaster, has met the difficult task of keeping the on-line information service up to date. BCS, who are taking over the job, will be hard-pressed to do half as professional a job.

Finally, to the stalwart John Mitchell, who has served 21 years on the various incarnations of IRMA from its early days of being the "Auditing By Computer" specialist group. John has undertaken and organised many IRMA

presentations, usually with his characteristic "in-your-face" approach, challenging all conventions. He has also been the editor of the highly informative and entertaining Journal for many years.

Three members have expressed a desire to remain on the committee:

Adam Carden, our most recent new committee member, joined at an earlier "critical/difficult" period, and has made membership activities and incentives a key issue.

Jean Morgan, our ever-reliable Treasurer, is a long-serving committee member and has always provided the fiscal information on time and in a very presentable form. More importantly, perhaps, she has always processed my expense claims quickly.

Finally, our Administrator, Janet Cardell-Williams, whom I recently described as our little bundle of energy, has always kept you, the membership, well-informed about up-coming events and, until the recent BCS changes, diplomatically reminded many members about their tardy responses to IRMA fee reminders.

Thank you once again, guys. I shall miss working with you all and trying to put the world to rights.

Finally ... the Membership

I should like to thank you all, the members, sincerely for your continuing support for the IRMA Specialist Group, for without you there would be no purpose, and what would we, the committee, be left with then? Just the buffet and the wine!

We love to hear from you – what you would like to see and what you would not like to see – and we take on board the often provocative challenges you raise at presentations and in the Journal, but hey … it's never dull!

My final plea is to consider a butchered version of John F Kennedy's 1961 inaugural speech: "Ask not what IRMA can do for you - ask what you can do for IRMA."

We need new people with new ideas and you are the ones to provide them.

Signing Off

So, as I ride off into the sunset after 5 years of committee membership, taking many fond memories with me, I can look forward to attending future IRMA functions without the stress-levels that accompany their organisation and, as a normal punter, to meeting many of you again.

I can also honestly say, that if you have enjoyed the last 5 years as much as I have … then I will have enjoyed it twice as much as you.

4. Treasurers Report

Presented by: Jean Morgan

There was a shortfall of expenditure over income for 2007/08 of £630.31, largely due to the loss of IRMA membership fees, but after this loss, the accrued balance held on account (at BCS) is a healthy £22,643.51.

Acceptance proposed by: Nighat Sheikh
Seconded by: Mark S Smith

5. Election of the Officers

As there are significant changes to the IRMA Committee, it was proposed that the composition of the Committee and the appointment of the individual officer positions, including Chair, would be discussed and confirmed by the Committee at their first meeting. The individuals holding the offices will be announced after the next committee meeting.

This spontaneous motion was:

Proposed by: Ross Palmer
Seconded by: Mark S Smith

It was agreed unanimously by all attending the AGM

6. Appointment of Committee

There were two nominations for new members of the Committee.

A motion to appoint all those (5) who sought committee membership was:

Proposed by: Ross Palmer
Seconded by: Jean Morgan

The motion to accept all those who volunteered to join the committee was passed.

The resultant 2008/09 BCS IRMA committee thus comprises, at this stage:

- Janet Cardell-Williams
- Adam Carden (in absentio)
- Jean Morgan
- Simon Paterson (new member)
- Theo Tryfonas (new member)

7. Motion to formalise IRMA name change

Motion: *To formalise change of name of the IRMA BCS specialist group, replacing "Audit" with "Assurance".*

This proposal had already received sanction of the BCS Specialist Group Executive Committee.

Proposed by: John Mitchell (in absentio)
Seconded by: Ross Palmer

The motion was passed.

8. Any other Business

There being no other business, the Chairman thanked all for attending and the 2008 AGM of the British Computer Society – Information Risk Management and Assurance Specialist Group was closed at 17:35.

THE BRITISH COMPUTER SOCIETY

			Budget totals 2007/08		Actual totals 2007/08
Cost Centre Budget Comparison	IRMA	Income	£2,795	Income	4,786.38
	As of April 30, 2008	Expenditure	£4,165	Expenditure	5,416.69
			£1,370	Shortfall	£630

Account	***Description***	***YTD Actual***	***YTD Budget***	***Variance***	***%***
Income					
1708	Events Registration Fees	3,891.38	1,720.00	2,171.38	126.24%
1903	Membership Subscriptions (SGs)	895.00	1,075.00	(180.00)	(16.74%)
	Total Income	4,786.38	2,795.00	1,991.38	71.25%
Expenditure					
3010	Travel/Subsistence (Other)	39.10	100.00	60.90	60.90%
4000	Stationery	1,204.66	1,600.00	395.34	24.71%
4130	Speakers expenses	579.59	290.00	(289.59)	(99.86%)
4150	Catering	1,356.36	975.00	(381.36)	(39.11%)
4210	Seminars & Conferences	1,078.05	(1,078.05)		
4212	Publicity & Materials	65.40	(65.40)		
4980	Administrative Services (SGs)	1,093.53	1,200.00	106.47	8.87%
	Total Expenditure	5,416.69	4,165.00	(1,251.69)	(30.05%)
Overhead Allocation (Charge)					
	Total Overhead Allocation (Charge)				
Overhead Allocation (Credit)					
	Total Overhead Allocation (Credit)				
Grand Total		(630.31)	(1,370.00)	739.69	53.99%

IRMA Reserves as at 30/4/07 £23,273.82

Information Technology Legislative Update

Dr A.Abimbola

NetHost Legislation

Abstract

NetHost Legislation, an Information Technology law Firm that assist companies create practical and strategic solutions to the challenges confronted by the increasing complex range of IT legislation statutes presented in this article:- recent developments in the field of European Union Data Protection Directive and its associated United Kingdom statutes and highlight recent changes.

1 Introduction

The Convention for the protection of individuals with regard to automatic processing of personal data which was signed by member states of the council of Europe at Strasbourg 28 of January 1981[1], and underpins most European data protection statutes. It was created to achieve greater unity between its members; extend the safeguards for the right to privacy, taking account of the increasing flow of personal data undergoing automatic processing. The Council of Europe ETS no108 provided critical definition, such as personal data- any information relating to an identified or identifiable individual (data subject); automatic processing – includes storage, editing operations if carried out in whole or part by automated means and automatic data file – any set of data undergoing automatic processing. These definitions are currently being used in national statutes of European member states like the United Kingdom.

The data protection statutes have been in existence for over four decades, while the first statutes were introduced in Germany other European member states followed suit. The implementation of member states data protection statutes have been mostly due to the compliance of the European Directive 95/46/EC[2], on the protection of individuals, with regard to the processing of personal data, and on the free movement of such data in addition to the Directive 2002/58/EC[3] also. Some European member states have decided to implement the minimal state of compliance with the European data protection Directive, thus adhering with minimum requirements. Nevertheless, other member states have agreed on a greater concept of data protection, seeking to elevate the interest and wishes of the individuals above those of data users.

In the subsequent paragraphs we discuss recent developments[4,5] within the data protection legislation.

2. European Union Data Protection Law Review

United Kingdom's Information Commissioner's officer (ICO) is currently inviting tenders to carry out a study into the strength and weaknesses of the European Union (EU) Data Protection Law[2]. Following the increasing public awareness and compliance breaches, concerns about the need for effective privacy safeguards and the pace of technology development, the ICO is keen to stimulate debate with hope of improving the data protection statutes.

We at NetHost Legislation believe that the following issues below should be considered in order to improve the Data Protection Statutes.

- New technological development such as development in data sharing, RFID systems, Biometrics, DNA ID systems and identity management systems have a clear impact on the requirement for data protection statutes. Also, the need for effective protection of the personal data of an individual can impose limitation on the use of these new technologies. Interaction is thus two sided: the technology influences the legislation and legislation influences technology. In addition, new guidelines would likely need to be recommended on how to implement the eight principles of the data protection statutes, in relation to these new technologies. And data subject would need to be informed on the composition and impact to their privacy the processes of these new technologies will have.
- Improvement of the implementation of the Data Protection Statutes itself: how to make the statutes more effective. A mix of policy instruments is needed for such an improvement varying from a better communication with society to statutes enforcement.
- Global privacy and jurisdiction issues, dealing with the external borders of the European Union need to be standardised. The jurisdiction of the Directive is limited to the territory of the European Union, whereas economic growth depends more and more on global networks outside the European Union. Companies based in the European Union increasingly outsource activities, including the processing of personal data to third countries. Moreover, recent cases like Swift[6] and PNR[7] confirm that other jurisdictions have interests in personal data originating from European Union.
- Data protection and law enforcement recent threats to society, whether or not related to terrorism have led to more possibilities for law authorities to collect, store and exchange personal data. In some cases, private parties, whom are not law enforcement authorities, are actively involved in the processing of personal/sensitive data. The eight principles of the data protection statutes need to be enforced and appropriate guidelines put in place.
- Raising awareness is a key issue in promoting a better implementation of the data protection statues, and this should be further exploited. Furthermore, exchange of best practice and harmonization within member states in the area of notification and information provisioning should be encouraged for cutting red tape, to reduce cost.
- Within the United Kingdom data protection statutes, personal and sensitive data protected during a person's life should not lose that protection privileges immediately upon the person's death. There should be a tolerance period, before a dead person's data loses data protection privileges, to enable their next of kin notify the data controller and appropriate actions taken.

- The definition and interpretation of the following phrases with the United Kingdom data protection statutes- "consent" and "explicit consent" found in the first article, also clarification is needed for the meaning of "relevant time", "disproportionate effort", "at the time" and "any further information" found at schedule 1. This will enable practitioners of the act to better understand and implement the statutes.

- In addition to the list of sensitive personal data included in the United Kingdom data protection act, the following could also be included- sensitive information, digital signatures, and financial data to protect individual privacy. In addition, thought should be given to information that covertly exposes sensitive data, such as, surname revealing a person's race. A consultation is needed to investigate if information that will reveal sensitive data covertly should be categories as sensitive data by the data protection statutes.

- Further more, compensation should be available for contravention of United Kingdom data protection statutes, which cause distress even if there is no damage. Also, the Information Commissioner should be empowered to carry out data protection "audits" without the consent of the data controller. This has recently been approved for government data controllers only[8]. Lastly, notification of breach should be made legally compulsory, thus the ICO will then be able to carry out audits and provide recommendations.

3. New Data Protection Close Circuit Television Code of Practice

United Kingdom's Information Commissioner's officer has recently issued a revised Code of good practice for Close Circuit Television (CCTV) operators aimed at striking that vital balance the individual's right to privacy and the public interest in security[5]. When CCTV is used to captured images that identify a living person, then it falls under the scope of the data protection statutes.

Below we summarise some aspects of the CCTV code of practice:-

- The code suggests carrying out an "impact assessment" to provide a basis of justification for using CCTV.

- The code covers what should be recorded, how the images should be used and to whom they may be disclosed

- CCTV images that fall under the statutes should be adequate and not excessive for their relevant purposes(s).

- Audio recording is justifiable only in extremely limited case and conversations of member of the public should never be recorded.

- The code addresses the fundamental issues of storage, disclosures and retention of images. A 30 day retention period was initially suggested, but more importantly, retention should not be longer than its necessary.

- Notice of operation of CCTV is required and should be displayed

4. References

[1] "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, 2008-01-07

[2] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", http://www.dataprotection.ie/viewdoc.asp? DocID=89, 2008-01-07

[3] "Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", http://www.dataprotection.ie/viewdoc.asp?DocID=71, 2008-01-07

[4] ICO Invites Tenders to Review EU Data Protection Law,http://www.ico.gov.uk

[5] Close Circuit Television Code of Practice, http://www.ico.gov.uk/Home/for_organisations/topic_specific_guides/cctv.aspx

[6] "SWIFT broke data protection law, says Working Party", http://www.out-law.com/page-7518, 2008

[7] "Passenger Data Deal Based on plan opposed by Privacy Regulator" http://www. out-law.com /page-7518,2008

[8] "Information Commissioner welcomes the government's commitment to strengthen the powers of the ICO", http://www.ico.gov.uk/about_us/news_and_views/press_releases.aspx?year=2007,2008

The Down Under Column

Bob Ashton

IRMA Oceania Correspondent

Readers may be familiar with an ATM fraud reported some years ago in which criminals took advantage of the long Christmas/New Year holiday taken by Scottish banks. During this period the normal monitoring of ATM withdrawal activity did not take place, and withdrawals were allowed to take place regardless of the balance on the account. A fraudster took advantage of this by withdrawing as much cash as he possibly could over a period of several days in central London for 3 years running. On the third year the Fraud Squad had anticipated the activity and were waiting to arrest him. These events were the subject of a BBC television documentary.

Similar activities have been documented on Australian television. In this case large numbers of otherwise impecunious citizens have been filmed filling shopping trollies at all night supermarkets, after they had discovered that the EFTPOS network was down. It is believed that opportunistic persons discovered that the EFTOS network was down as the stores were observed to have reverted to manual processing for EFTPOS payments, and were already aware that because of this, normal controls on withdrawals from overdrawn accounts did not apply. They quickly informed friends and associates of this state of affairs which led to a shopping bonanza.

In a new twist on this theme Australian criminals have taken to cutting fibre optic cables supplying shopping centres in order to facilitate this type of fraud. A group of men dressed in reflective safety vests to look like maintenance staff was recently seen "working" at a cable pit in Western Sydney. Two fibre optic cables were cut, and it is believed by Police that the purpose was to disable the EFTPOS machines in the Westpoint shopping centre in Blacktown, which would cause the shops to resort to

manual transactions. It is believed that the same gang was responsible for 5 such cuts in the previous 6 weeks.

In this instance the EFTPOS network in the targeted shopping centre was not affected, and a spate of fraudulent purchases was fortuitously avoided. Shop owners were, however, warned not to use manual transactions that day.

The severed cables caused huge collateral damage, however, including 10,000 homes loosing phone and internet access and cell phone base stations, broadband services and data lines, including critical infrastructure, being affected over a wide area. A team of 30 technicians was required to work throughout the night to restore services.

The above facts have been widely reported in Australian media. In many countries the service pits for these cables are clearly labelled and easily identifiable and accessible making them an obvious target for criminals and others.

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.

HUMOUR PAGES

DEFINITIONS

BULL MARKET – A random market movement causing an investor to mistake himself for a financial genius.

BEAR MARKET – A 6 to 18-month period when the kids get no allowance, the wife gets no jewellery, and the husband gets nothing.

MOMENTUM INVESTING – The fine art of buying high and selling low.

VALUE INVESTING – The art of buying low and selling lower.

P/E RATIO – The percentage of investors wetting their pants as the market keeps crashing.

BROKER – What my broker has made me.

STANDARD & POOR – Your life in a nutshell.

STOCK ANALYST – Idiot who just downgraded your stock.

STOCK SPLIT – When your ex-wife and her lawyer split your assets equally between themselves.

FINANCIAL PLANNER – A guy who actually remembers his wallet when he runs to the 7-11 for toilet paper and cigarettes.

MARKET CORRECTION – The day after you buy stocks.

CASH FLOW – The movement your money makes as it disappears down the toilet.

YAHOO – What you yell after selling it to some poor sucker for $240 per share.

WINDOWS 2000 – What you jump out of when you're the sucker who bought Yahoo @ $240 per share.

INSTITUTIONAL INVESTOR – Past year investor who's now locked up in a nuthouse.

PROFIT – Religious guy who talks to God

SETTINGS FOR YOUR AUTO RESPONDER

- I am currently out of the office at a job interview and will reply to you if I fail to get the position.
- You are receiving this automatic notification because I am out of the office. If I were in, you very likely would have received nothing at all.
- Sorry to have missed you, but I'm at the doctor's having my brain and heart removed in preparation for promotion to our management team.
- I will be unable to delete all the emails you send me until I return from vacation. Please be patient, and your mail will be deleted in the order it was received.
- Thank you for your email. Your credit card has been charged £5.99 for the first 10 words and £1.99 for each additional word in your message.
- The email server is unable to verify your server connection. Your message has not been delivered. Please restart your computer and try sending again. (The beauty of this is that when you return, you can see who fell for it, perhaps repeatedly.)
- Thank you for your message, which has been added to the queue. You are currently in 352nd place, and can expect to receive a reply in approximately 19 weeks.
- Hi, I'm thinking about what you've just sent me. Please wait by your PC for my response.
- I've run away to join a different circus.
- I will be out of the office for the next two weeks for medical reasons. When I return, please address me as 'Lucille' instead of "Ted."

EVOLUTION OF BRITISH MATHEMATICS TEACHING 1970-2008

1. **Teaching Maths In 1970**
   A logger sells a truckload of timber for £100.
   His cost of production is 4/5 of the price.
   What is his profit?

2. **Teaching Maths In 1980**
   A logger sells a truckload of timber for £100.
   His cost of production is 4/5 of the price, or £80.
   What is his profit?

3. **Teaching Maths In 1990**
   A logger sells a truckload of timber for £100.
   His cost of production is £80.
   Did he make a profit?

4. **Teaching Maths In 2000**
   A logger sells a truckload of timber for £100.
   His cost of production is £80 and his profit is £20.
   Your assignment: Underline the number 20.

5. **Teaching Maths In 2008**
   A logger cuts down a beautiful forest because he is selfish and inconsiderate and cares nothing for the habitat of animals or the preservation of our woodlands.

   He does this so he can make a profit of £20.

   What do you think of this way of making a living?

   Topic for class participation after answering the above question: How did the birds and squirrels feel as the logger cut down their homes?
   (There are no wrong answers.)

Application Form for Affiliate Membership

Surname/Last/Family Name	First Names	Title (Mr/Mrs/Ms etc)	Date Of Birth (DD/MM/YY)

Home Details	**Work Details**		
Address	Organisation Name		
	Department		
	Address		
Town/City	Town/City		
Postcode	Postcode		
Country	Country		
Telephone	Telephone		
Telephone (Mobile)	Communication Preference? (please tick)	By Email	By Post
Contact Email	Alternate Email		

What prompted you to make this application at this time? Please choose an option from the list below:

Press Advert ☐ BCS Website ☐ Other Website ☐ BCS E-Mail ☐ Railway/Underground Advertising ☐

University department/lecturer ☐ Employer ☐ BCS Event ☐ BCS Leaflet ☐ Exhibition ☐ Other ☐ Colleague ☐

BCS Member ☐ Press Publication ☐ BCS Presentation ☐ Search Engine Advertising ☐

Payment Details and Method of Payment (price valid for the year ending 30th April 2008)

The annual subscription for BCS affiliates is £25.00. You can pay by cheque, credit card or debit card*.

☐ **Cheque** Please make cheques payable to The British Computer Society

☐ **Credit/Debit* card** (please circle your choice) Visa / MasterCard / Switch (Maestro) / Debit Card (*Not Solo) / American Express

Name and initials as shown on card _____

Credit / Debit* Card number _____

Start date: _____ Expiry date: _____ Issue No. (if Switch Card): _____

COMMUNICATING WITH YOU

We keep the personal information you give us to help provide you with the services you require from the British Computer Society (BCS).

We may also pass on your details to our partners or approved suppliers who may contact you about their products. You can opt out of this by ticking the box ☐

For the full privacy notice, or for access to or correction of your personal information, go to the privacy notice on our website at www.bcs.org or contact: BCS Customer Service department on 0845 300 4417 (UK) or +44 (0)1793 417424 Fax: +44 (0)1793 417444
Email customerservice@hq.bcs.org.uk

DECLARATION

I wish to join The British Computer Society as an Affiliate. I confirm that, if accepted I will be governed by the Society's Charter, Bye-Laws and Regulations from time to time in force and will abide by its Code of Conduct from time to time in force. I will maintain the dignity and welfare of the Society, conduct myself honourably in the practice of my profession and will observe the provisions of the BCS Code of Good Practice from time to time in force.

Signature _____ **Date** _____

TO JOIN IRMA YOU MUST BE AT LEAST AN AFFILIATE MEMBER OF THE BCS.

PLEASE EITHER COMPLETE THIS FORM AND SEND IT TO: BCS IRMA, 47 Grangewood, Potters Bar, Hertfordshire, EN6 1SL

OR

Apply on-line at www.bcs.org.uk

Once you have ben accepted into the BCS you will be able to select IRMA as one of your Specialist Groups or branches.

Once completed please return to:

BCS Membership Operations Department, First Floor, Block D,
North Star House, North Star Avenue, Swindon SN2 1FA United Kingdom
Tel: 0845 300 4417 (UK) or +44 (0)1793 417424 Fax: +44 (0)1793 417444

BCS IS A REGISTERED CHARITY. NUMBER 292786

MTG/FORM/303/0407

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

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	TBA
SECRETARY -	TBA
TREASURER -	Jean Morgan
MEMBERSHIP SECRETARY -	Adam Carden
JOURNAL EDITORS –	Mike Lavine & Rob Melville
CURRENTLY WITHOUT PORTFOLIO	Simon Paterson
CURRENTLY WITHOUT PORTFOLIO	Theo Tryfonas

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

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