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

JOURNAL
VOLUME 17 NUMBER 2 SUMMER 2007 ISSN 1741-4229

BCS
THE BRITISH COMPUTER SOCIETY

Programme of Briefings & Meetings 2007

Date	*Subject*	*Speaker*	*Time*	*Location*
6 Feb 2007	Search Engine Hacking	Peter Wood	16.30	BCS London Office
6 Mar 2007	Changing the value perception of security	Des Ward	16.30	BCS London Office
3 Apr 2007	Control Self Assessment as an Audit Tool	John Mitchell	16.30	BCS London Office
1 May 2007	AGM & Using Software for Risk Based Auditing	Trevor Williams	17.00	BCS London Office
5 Jun 2007	Mobile Devices and Network Security	Stan Dormer	16.30	BCS London Office
3 Jul 2007	IT Assurance	John Mitchell	16.30	BCS London Office
19 Jul 2007	Configuration Management Horror Stories (Joint meeting with Configuration Management SG)	John Mitchell	17.30	BCS London Office
9 Oct 2007	Computer Crime Update	Peter Wood, Daniel Cuthbert Sarb Sembhi, John Mitchell	Full Day	BCS London Office
6 Nov 2007	Forensics TBA	TBC	17.30	BCS London Office
11 Dec 2007	The Criminal Mind	TBC	17.30	BCS London Office
8 Jan 2008	TBA	TBC	17.30	BCS London Office
5 Feb 2008	TBA	TBC	17.30	BCS London Office
14 Feb 2008	Software Auditing (Joint meeting with the Advanced Programming SG)	John Mitchell	17.30	BCS London Office
4 Mar 2008	TBA	TBC	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 **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

The Government keeps trying new schemes to persuade us to vote.You can see their concern.If a government is elected by only one-third of the electorate, then it cannot really claim to have a mandate to govern.The answer, the Government believe, as do the opposition, is to use technology.The internet, SMS texting and interactive television are in the frame and various pilots are tried at each election.Now increasing the turnout is a laudable objective in its own right, but not at the expense of the integrity of the process.The Government has already had its fingers burnt with postal voting, but still has not learned that confidentiality and integrity are at least as important as availability.I have both a personal and professional interest in this area and for a couple of years I was the BCS's resident expert on the now disbanded Security Panel.Since then I have kept up the pressure on the Government, via the Electoral Commission, who are meant to ensure that the voting process is fair.Every time they try something new they ask for comments on the process and I examine it and have always gone back with the same observation.'Yes, the process may encourage more people to vote, but it is inherently insecure'.They thank me for my interest and then we go through the same farce the next time around.Public consultation I have learned is simply a way of legitamisingwhat was always intended.A bit like the electronic petitions on the Number 10 web site.Yes, we realise that over a million of you disagree with road pricing, but we are going ahead with these trials anyway.I tried postal voting this time round.When I received the ballot paper it included a telephone number so that I could check if my vote had been received.Excellent, I thought, until after several days of trying the national rate number for what should have been a local call, the system kept telling me that my vote had not been received.Eventually I called my local electoral services officer who said that my vote had been received, but that they did not have the resources to scan the information into the system.My letter of complaint to my council received a brush-off response along the lines that we are too busy, we received a lot of postal votes, we outsourced it and scanning takes time.No apology, no mentioning of improving the service.Nothing either so far from the Electoral Commission, but perhaps they are too busy thinking up new schemes.

Then Tesco sent me an email saying that my internet phone number will be discontinued unless I use it within the next thirty days.As I use the device regularly I contact their support desk to ascertain what the problem was.There is no problem I am told,We simply sent this to everyone as a friendly reminder to ensure that people use the phone.So Tesco's idea of a friendly reminder is to threaten all their customers with disconnection.I would hate to receive an unfriendly message from them.I wonder how these things happen.Does someone sit around all day thinking of ways to annoy their customers, or they so lazy that they can't be bothered to filter out their users?Either way, it shows that the old audit test of monitoring customer response is a sure way of ascertaining how well your customer service is performing.If for every complaint you assume that a further ten customers must be really annoyed, but do not have the time or energy to do anything, then implementing a simple report to the main board should focus their minds on the link between customer service and customer loyalty.Although as a senior banker once told me when his cups one evening, "John, you have more chance of getting divorced than changing your bank account, so why should we concern ourselves with customer service"?.He is right of course.There has to be a business need to provide good customer service.If the customers don't ask for it then why provide it?

This is why I have recently got myself elected to the Specialist Group Executive Committee (SGEC).I was incensed at new BCS accounting rules which effectively removed from the SGs their reserves.In our case over £20,000 of hard earned money has disappeared into BCS central funds.See our Treasurer's report in this edition.However, what really annoyed me was the BCS attempt to rewrite history.Some of us are old enough to know that the SGs saved the BCS from bankruptcy in the early 1990s, but the current BCS line is that this did not happen.The job of the SGEC is to represent the SGs, but I saw very little of that in this instance.So putting my feet where my mouth was I had no option but to get involved once again in BCS central affairs.I have previously been a member of Council and was once asked to be BCS Treasurer so I do have some idea as to how things should work.That's what we need from you.More

involvement in running your SG.If you don't get involved then you can't complain about what your Management Committee delivers.

In this issue we have a suggested charter for system administrators from our old friend Andrew Cormack of UKERNA (United Kingdom Education and Research Networking Association) which is an attempt to codify the duties of these powerful people.Toby Stevens, chair of the BCS Information Privacy Expert Panel, identifies identity myths, analyses identity management and proposes that there's no such thing as identity theft.Ben Richmond discusses using enterprise content management (ECM) to enable the knowledge-based workforce, while, despite all the theory, the European Spreadsheet Users Interest Group (EuSprig) shows how spreadsheets are really created.A new, regular column from Andrea Simmons of the BCS Security Forum who identifies the various consultation exercises it has been involved with, plus our usual report from the antipodes by Bob Ashton and an update on membership benefits from Mark Smith.Check out our accounts from Jean Morgan and you will appreciate my point about kissing our reserves good bye. My goodness, I am becoming a really grumpy old man.

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)

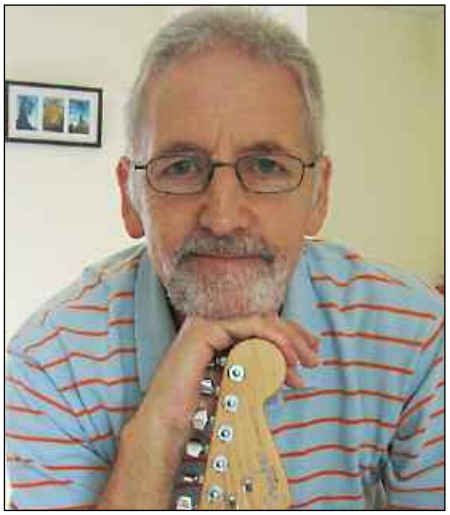
Events

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



Greetings, Readers

"I read the news today, oh boy …"

Thus goes the celebrated opening line of "*A Day In The Life*", from the landmark Sgt Pepper album, which is 40 years old this summer (can you believe that?) and still selling strongly.

However, the "news today" (April 23rd – St George's Day) refers not to "four thousand holes in Blackburn, Lancashire" but "one hundred million litres of sewage in the Firth of Forth" which, try as I might, is a phrase that does not easily scan into the rhythmic meter of the song.

Apparently, a catastrophic pumping station failure allowed this quantity of partially diluted sewage to flow freely into the famous waterway over a period of 3 days. (To get this into perspective, this is enough to fill 170 Olympic-sized swimming pools, which is an unpalatable comparison for the keen swimmer to take on board, I guess.)

The water company's head of corporate affairs apologised to customers for the inconvenience caused (which is nice) and added that "on investigation our engineers found the repair was a much larger operation than first anticipated and we have had to locate specialist pumps from other parts of the UK".

So, I wonder, from a risk perspective, what lessons can be learned from this, apart from don't swim with your mouth open?

For a big-profits company like that, you'd think the preventive no-brainer would be investing in a little critical on-site "duality" of the pumps, wouldn't you?

I'd love to have been a fly on the wall when the water company was carrying out its risk/business impact analysis, simply to observe which stakeholders were involved. Were representatives from the general public and environmental experts present? Or did it comprise just business leaders in the company looking after the bottom-line for their Australian owners (who should be glad this didn't happen in Sydney Harbour)?

Ah well, we can all be wise after the event, I guess, and I am no exception, having put a power drill through the middle of a water pipe more than once in my life!

The ants …

In business continuity and disaster recovery terms, we could all take a few lessons from the natural world. Take a look at ants, who are the absolute masters of BCP/DR.

Only this weekend, lifting a slab in the garden, I encountered thousands of the little guys 'n' gals implementing their well-rehearsed BCP, scurrying around, lifting huge eggs (ant eggs, that is) and, like one cohesive organism, ultimately removing the lot within 3 minutes to the safety of the lower tunnels.

Later the same day, I happened to dump a bag of compost on to my cherished raised vegetable bed and, too late, found another ant's nest in the contents! You'd think this would be the end for them, wouldn't you, but no … by the end of the afternoon, they had recognised adversity as opportunity and colonised this lush new environment!

Horatius, he say …

BCP is nothing new. Horatius, the Roman poet (65 - 8 BC, which must have been confusing for pension planning, getting younger and younger like that), was a profound pundit on the subject when he said: "It is your business when the wall next door catches fire."

However, it was also Horatius who said, "Enjoy today, putting as little trust as possible in tomorrow!", so maybe his BCP testing plan was not turning up particularly encouraging results.

BS 25999 …

All of this brings me effortlessly to BS 25999, the new British Standard Code of Practice for Business Continuity Management (BCM), which I have recently purchased.

I can't say there is anything new in this publication that cannot be learned elsewhere, but it DOES have it all in one place, including an overview of BCM, managing the programme, understanding the organisation (including business impact analysis), developing, implementing, exercising (which we would probably call "testing"), maintaining and reviewing the strategy.

It is closely related to ISO 27001 and has the potential to become the definitive BCM standard for organisations and their clients. While £90 + VAT seems a bit steep for 50 pages (that's £2 a page – including the blank one), it is eminently readable and presents the concepts in an easy-to-assimilate style.

Wi-fi safety concerns …

Also in the news today is a claim by a teacher's union that wireless computer networks in schools should be investigated over any possible health risks to children and staff.

The Professional Association of Teachers has called on the Government to look into concerns about radiation emitted by the equipment after one of their members complained of health problems when wi-fi was installed in his classroom last September.

Is this lining up to be the next "mobile phone masts"?

Well, take care and have an enjoyable summer.

Does the Board Know?

Ben Richmond

Using enterprise content management (ECM) to enable the knowledge-based workforce is the key technology trend for the next five years. But it will take strategic, board level commitment to make it work, insists Ben Richmond, chairman and managing director of The Content Group.

Within five years every employee will expect the rapid provision of tailored information to support day to day roles. They simply will not countenance the confusion and inconsistency of information resources endured today as organisations struggle to manage multiple sources of unstructured data.

Making that shift, however, requires buy-in at board level. Isolated implementations of ECM technologies without a joined up strategy - from email management to document scanning - will address immediate business issues and reduce costs, but they will not alone deliver the true knowledge-based organisation.

It will be a strategic, board level approach that provides a fundamental, strategic change towards a process and people-led information infrastructure that enables real business transformation.

Bad news

Despite the maturity of the IT industry, it is still the bad news stories that typically get board level attention. And today the story revolves around information costs: from the cost of achieving compliance to the escalation in storage costs as IT struggles to manage unparalleled multiple sources of unstructured data.

Indeed, it is becoming patently clear that the 'store everything' policies designed to address compliance requirements are failing. They are adding untenable cost and, more often than not, failing to deliver the audit, accountability and information access actually required to comply with multiple regulations.

But for any beleaguered IT director, getting the attention of the top brass is actually a massive opportunity. Data storage can, and should, be about far more than retaining huge quantities of data simply to satisfy bureaucrats and politicians. It should be about leveraging the vast array of structured and unstructured information now available, from email to websites, drawings to presentations.

Instead of leaving employees floundering in a mass of uncontrolled, unaudited and unmanaged information, the true knowledge-based organisation provides an effective and productive working environment.

Turning the tide

That goal will never be achieved, however, if organisations persist in solely an IT-led, data specific, attitude towards information management. Implementing an email management solution may patch over the cracks in one aspect of the business but it will not achieve the knowledge-based organisation.

The good news is that such email solutions can be incorporated into an overall ECM strategy but only if the organisation is willing and able to admit there is a bigger problem than managing email overload.

The real issues are business-led. How can the organisation manage the bid process more effectively? How can people who span the globe get access to the same project information? How can business processes be automated and controlled?

It is the effective, business-driven management of structured and unstructured data that should be driving ECM investment - not a desperate bid to address storage costs or purely to reduce paper. Which is why the ECM strategy has to be driven at board, not IT or departmental, level.

Cultural change

Once the global ECM strategy has been defined, organisations can prioritise key areas of the business to achieve quick wins, it does not have to be a 'big-bang'. It can then be achieved in a phased approach whilst ensuring it follows the joined up thinking of the bigger picture.

Critically, the approach is business - not data type–led. In bid management, for example, organisations need to identify who is involved - both within the organisations and across the supply chain; what content is required, from drawings to email, specifications to hard copy documents; and what compliance challenges need to be considered.

The organisation can then use ECM technologies to ensure the right content is available to the relevant individuals in the most appropriate fashion. The entire information life cycle is tracked to provide visibility of revisions and compliance accountability. The process is smoother, more efficient and individuals have immediate access to the information required to enable the bid process, irrespective of data type or source.

Compare this to the quick fix to the email problem. Email is simply a medium to communicate bids. For any organisation looking to maximise the bid management process, imposing greater email control will have no effect whatsoever, it is purely an IT-led requirement. Yet addressing email as part of the overall ECM deployment will also deliver the benefits initially identified by the IT department.

Furthermore, underpinning the success of every ECM deployment is cultural buy-in. If there is no demonstrable value to an individual employee, no improvement in information value, and no return on investment for each business area, the technology simply will not be adopted. And the organisation will continue to struggle with multiple versions and lack of control over unstructured data sources.

Information vision

Once an organisation has deployed ECM strategically across the business, it can embark on a completely new way of working. Individuals have the relevant, meaningful information required to be more productive. There will be no time

wasted searching for information and trying to build knowledge.

Knowledge will be tailored to every individual to enable collaboration and interaction, to remove geographic boundaries and support the evolution towards truly client-centric business. Furthermore, the technology will ensure compliance as part of the inherent processes for information creation, collaboration, storage and retrieval, further reducing the burden on employees to remember to follow the right corporate processes.

With the right ECM infrastructure in place, content can be geared around process and how people interact with the business, providing every employee with the information required to do the job well. Indeed within a few years such information provision will be as standard a part of corporate life as is the web site today.

Good news

Getting the attention of the board is the first step in transforming a massive IT headache into a seriously good news story. It presents a chance to evolve the ECM deployment beyond the IT-led solution, addressing key points of pain in a bid to reduce the storage overhead, compliance and information management costs.

Taking the bigger picture approach and embarking on a business-wide ECM strategy delivers incremental wins to each and every part of the organisation. Critically, it is the essential step in creating a true knowledge-based organisation.

Ben Richmond is one of the UK's leading experts on ECM.

The Content Group
Content House, St. James's Place.
Cranleigh, Surrey GU6 8RP

Tel: +44 (0)1483 275588
Fax: +44 (0)1483 273855

Email: info@thecontentgroup.co.uk

Membership Matters!

Adam Carden

At the recent AGM, our chairman announced a fall in membership from last year. A declining membership could mean an uncertain future for our specialist group.

I ask all of our members to encourage their colleagues in the audit and risk management fields to join our group and reap the benefits that membership of IRMA brings. And, if you are reading this issue of the journal and you are not a member of IRMA, come along to one of our events and see if you would like to join.

Membership of IRMA is not without benefits. In addition to the interesting series of seminars run throughout the year on topics as varied as Search Engine Hacking and Risk Based Auditing, members of IRMA can also benefit from:

- a free quarterly journal which keeps members in touch with advances in information systems control and audit techniques;
- 20% off All Unicom events;
- 20% off IACON;
- 15% off CISO Summit;
- 15% off Websec;
- 10% off E-Tec courses;
- 20% off Wizrule and Wizwhy data mining, data auditing and cleansing tools; and
- 15% off IDEA and Caseware Examiner for IDEA

It was also decided at the AGM to make IRMA membership free for BCS members in a bid to encourage more BCS members to join our group.

Adam is IRMA's Membership Secretary

Identity, identity, identity

Toby Stevens

Toby Stevens, chair of the BCS Information Privacy Expert Panel, identifies identity myths and analyses identity management. And there's no such thing as identity theft....

Each of us carries and uses a wealth of cards, badges, certificates, passwords, PIN numbers and other identifiers. Each time we transact in a shop, online, or with the state, we have to prove who we are all over again, and each time we do so, we have to give away yet more of our personal data.

Furthermore, all of these different identifiers are effectively pseudonymous; my bank has no mechanism to prove that the Toby Stevens who holds this credit card is the same Toby Stevens who has this National Insurance Number or this frequent flyer card.

These different personas can effectively grant me a degree of privacy, since the data is not shared between the organisations, and I'm the only person who can prove that we are one and the same.

However, pseudonymity also means that companies - and the finance sector in particular - need to take steps to protect themselves, and hence why we require the likes of credit reference agencies to take a very educated guess at the relationship between these personas. This process is expensive and error-prone.

Governments have the same problem. We invest huge sums in data sharing, data matching and longitudinal studies to try to deal with the fact that we don't have a single trusted view of the citizen.

The citizen, on the other hand, needs to reassert his or her identity time and again when dealing with different parts of the state. Clearly this is not an efficient state of affairs. We neither have identity, nor management of it.

So what is identity management?

The goal of identity management is therefore to simplify this process for the benefit of all parties concerned, and to help support the trust relationships between those parties.

However, that's where our shared understanding of identity management comes to an end. Consultants talk in terms of business process re-engineering and single customer view.

Technologists focus upon the mechanisms needed to bring together network protocols and application interfaces. Governments dwell upon the need for database repositories, data sharing and identity cards.

I personally prefer to think of identity management as:

'The provision of systems and controls that can determine the entitlement of an individual or machine to transact within an environment, and assign limits of liability in the event of a transaction failure.'

When it is reduced to its base functions, the purposes of any identifying scheme are two-fold: to establish the eligibility of each party to conduct a transaction, and to assign the limitations of liability in the event of a failure.

Without eligibility and liability, we cannot achieve trust between the two parties. And that, surely, is the purpose of identity management. Except that identity management is probably not the right phrase to describe what we are doing.

Why identity management is the wrong phrase

We talk about identity management as a catch-all to describe the process of finding out who someone is. But if someone is trying to pass through immigration, we don't care who they are, simply whether they are entitled to do so.

If the passenger on the plane next to me is acting in an odd manner, I don't care who he is, but whether he has terrorist intent. A shopkeeper doesn't care who I am, simply whether my credit card transaction is valid.

A supermarket, of course, takes a far greater interest in me, since it has complex marketing mechanisms that revolve around identifying its customers. But its computers don't care who I am, they are there to generate the most efficient and complete marketing profile that they can obtain.

Nor are we trying to 'manage' that identity: normally, we are in fact trying to answer one or more of three questions:

- The first is: who is this person? Can we find them within our system?
- The second question is: is this person unique within the system? In other words, are they trying to claim more than one persona?
- Finally: is this person who they claim to be? Can we reliably prove that they are the legitimate holder of the credentials that they have presented?

This problem is compounded by misrepresentation of identity theft. Identity theft does not exist: you may abuse or misuse my identity, but you can't actually strip me of it.

Elements of the media, industry and the state have all at one time or another gathered crimes under the banner of identity theft for the sake of convenience.

There are certainly some very unpleasant crimes that depend upon collecting and misusing personal information, but they are not theft of identity. 'Data rape' might be a more accurate (if unpleasant) way to describe the violation of personal information.

When we confuse these concepts under the catch-all of identity management or identity theft, we also confuse the citizens/customers to whom we are trying to sell the benefits.

The imbalance of benefits

And it is here that we run into real problems. In nearly every case, the bulk of the benefits are delivered to the state or organisation through improved efficiency and reduced fraud, not to the

law-abiding individual. As a citizen I don't want to have my identity managed by the state or a private company, I want to retain a strong degree of control over it myself.

I want some assurance that it will be protected against those who wish to misuse it, and that if that happens, that I will have some means to obtain redress and set the record straight quickly and easily. Let's stop talking about identity management, and start thinking in terms of identity assurance.

Identity, privacy and security

Another popular misconception in this field is that identity assurance is the enemy of privacy and security - that if we can be identified then we will sacrifice our privacy, and that the data can never be kept secure. This simply isn't true.

With a strong identity mechanism in place, we can protect our personal data and disclose less - not more - personal information about ourselves. Federated identity schemes do away with the requirement for massive databases, and allow the citizen to determine where their data is stored and how it is used.

Organisations such as Liberty Alliance and Microsoft have developed principles, architectures and products that deliver both strong identity and strong privacy. Both of these are essential in the information age.

How biometrics work

Whilst we are talking about identity, it is worth saying a few things about biometric technologies, since these are so commonly incorporated into identity assurance schemes. Biometric technologies are an invaluable mechanism to protect and support identity assurance. But let's set the record straight about some of the popular misconceptions.

Biometrics are not secrets. We leave a trail of biometrics everywhere we go, through our fingerprints, recordings of our voices, pictures of our faces, even samples of our DNA.

Biometric technologies are not 100 per cent accurate - they use pre-determined risk thresholds to determine whether to trust the biometric or not. The highly reliable thresholds achievable in a controlled environment are not the same as those used 'out in the wild' with real people in real environments.

And, most importantly, there is the difference between biometric images and biometric templates. An image is a copy of the biometric, for example an exact reproduction of a fingerprint or a face. A template, however, is a one-way mathematical function that describes key characteristics of the image.

For example, in a fingerprint, it describes where the key attributes of the fingerprint are. It is the template that is used to recognize the biometric. The image cannot be reconstructed from the template; in other words, if you have the template you do not have a copy of the biometric itself.

When civil liberties campaigners protest about fingerprinting before an individual has been charged with an offence, often their concern is that the systems are unnecessarily capturing an image of the fingerprint and enrolling that into the database, when all that is actually required is to generate a template and see if it matches any of the images already in the database.

Private-sector identity assurance schemes generally eschew recording an image, since this provides a valuable target for attackers.

Once we stop treating biometric technologies as a panacea, and design systems that recognise that biometrics are not private; that they are not always accurate; and that we do not need to record a biometric image every time we check a biometric; then we will achieve public acceptance and ambient use of biometrics far faster and more effectively than we have to date.

The citizen data substrate

So what is the point of all this? What could we achieve if we took a radical new approach to identity? If instead of engineering identification systems to serve the needs of the state, we started to build for the needs of the citizen?

To my mind, the holy grail here is what I'll call the 'citizen data substrate', a bedrock of highly distributed data upon which both government and commercial systems could be built. This is not a single database, nor even a number of shared databases, but a massively distributed, federated layer of data that can be accessed by citizens, state and industry alike.

Individuals can determine what data is stored in the substrate, and where it is stored: some might be in government-owned databases, other elements might exist only on smartcards in their wallets. The substrate can accommodate the privacy wishes of those who trust the state with their data and those who do not.

The citizen substrate would allow us to do away with the need to build and populate massive databases.

It would create an environment where government, commerce and citizens not only trust the government's identity services, but wish to build and use value-add applications based upon them.

It could massively reduce the long-term cost of delivering citizen-centric systems.

The technology to put this vision into practice already exists, and is in commercial use today. What we require now is the political will to set aside some of our existing ideas and misconceptions, and to put this into practice.

Toby Stevens is chair of the BCS Information Privacy Expert Panel, and director of the Enterprise Privacy Group. The views in this article are his own, and do not necessarily reflect those of the group's member organisations.

Toby Stevens FBCS
Director, Enterprise Privacy Group /
Deputy Chair, BCS Security Forum
59, High Street, Odiham,
Hants, RG29 1LF
T: 01256 702325
M: 07796 698949
toby.stevens@privacygroup.org

IRMA Accounts as at May 2007

Jean Morgan – Treasurer

Income & Expenditure Statement – AGM 1/5/07

Overall, we have reduced our in-year deficit from nearly £3,000 last year to under £500 this year, which is good.

The table below shows this financial year and last year for comparison.

BCS policy for SG accounting is changing – to exclude SG reserves.We will continue to maintain an account of our reserves pending clarification of the position.

		1/5/05-30/4/06	1/5/06-30/5/07	
Opening balance 1 May		25,588.69	23,765.28	Interest added to Reserves
Account	***Description***			
Income				
1903	Subscriptions Income	3,467.00	1,450.00	Reflects Chairman's report of reduced membership numbers
1970	Events Income	1,915.03	2,359.52	Bulk of this was from joint event with ICAEW
	Total Income	5,382.03	3,809.52	
Expenditure				
3090	Meeting Expenditure	783.41		
4000	Stationery & Printing	4,709.21	1,486.67	Reflects move to electronic Journal
4100	Postage & Telephone		32.82	
4120	Travel Expenses		60.53	
4130	Speakers Expenses		158.90	
4150	Catering	724.19	819.12	
4200	Publicity & Marketing		294.65	Speakers' gifts pre-purchased
4212	Events Expenditure	338.38		
4915	Sundry Expenditure	74.00	111.60	
6000	Committee Expenditure	828.05	347.55	
6100	Administration	911.05	989.14	
	Total Expenditure	8,368.29	4,300.98	
Grand Total		(2,986.26)	(491.46)	
		22,602.43	**23,273.82**	

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

CITRIX SECURITY

Citrix technology has become ubiquitous in recent years as organizations take advantage of the benefits of this thin client model, including:

- Lower desktop management costs – client software can be managed centrally and end users do not have the opportunity to alter configurations.
- Lower hardware costs - thin clients are cheaper than PCs and old PCs can be used for years after they would have become obsolete under the Windows product life cycle.
- Thin client security – users do not have the opportunity to introduced malware or remove data as thin client devices do not provide removable media facilities.
- Enhanced resilience – client software is rebuilt every time the user logs on.

The current widely encountered generation of this architecture typically consists of a combination of Windows Server 2003 and Citrix Presentation Server 4.0.

Auditors seeking guidance on how to provide assurance that this layer has been properly secured have had little available to them until recently.

A welcome addition to publicly available resources is a recent Global Information Assurance Certification (GIAC) Global Security Essentials Certification (GSEC) Gold Certification paper by Shane Wescott, available in the SANS Institute Reading Room at www.sans.org. The paper covers the following areas:

1. General description of. Citrix Presentation Server concepts.
2. Server hardening
3. User profile security and lockdown
4. Application security and lockdown
5. Auditing and monitoring

The paper puts Citrix Presentation Sever hardening into its proper context by providing brief descriptions of the processes required to harden Citrix's Windows environment, in respect to Windows 2003 Server hardening and Windows 2003 Terminal Services hardening. Auditors wishing to get off to a quick start in this area will find the checklists provided particularly useful.

A major benefit of Citrix, which is not mentioned in the Paper, is the fact that traffic between the server and user terminals can be encrypted using 56 or 128 bit encryption. This process is enabled by simply clicking 2 boxes and the auditor should always be satisfied that this obvious precaution has been taken.

A more detailed checklist on securing Windows Terminal Server and Citrix Presentation Server can be found at: www.sessioncomputing.com/security.

A description of the purpose and use of Microsoft's Security Configuration Wizard, in the form of an article entitled: "Securing your Terminal/Citrix Servers with the Security Configuration Wizard" can be found at www.terminalservices.org. The Wizard is freeware and is designed to lead an administrator through the process of setting up Windows Server 2003 in a secure manner, in this context the Windows Terminal Server/Citrix server environment. It works by scanning the server to see what role or roles it has. Then it determines what the minimal software requirements for that role or role are and allows everything else to be disabled. Clearly an auditor will gain comfort if this process has taken place. The results of this process can be uniformly applied to secure all the units in a Citrix server farm, where this is appropriate.

Security Forum Strategic Panel

Andria Simmons

The BCS Security Forum (SF) is going from strength to strength so I thought I would take this opportunity to update you. The BCS Security Forum is working collaboratively with a number of interested parties and will be moving forward this agenda with ISC2, Cyber Security KTN and IISP in the coming months.

There is a great deal that the BCS SF is asked to contribute on or attend. I am sure that a lot of this is being passed on to you all via your Chair or equivalent. Please do feel free to be involved as the more we co-ordinate and contribute, the stronger the voice of the BCS SF and the more likely it is to be seen as a source of knowledge and expertise on a wide range of security related issues.

Consultations

For example, the BCS Security Forum has been asked to contribute to the following consultations:

Title	Submit To	Status	Deadline
The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State	Select Committee on the Constitution, House of Lords	Open for comment;	12noon, Fri 25th May 2007
Retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks	Home Office	Open for comment;	12noon, Fri 25th May 2007
A Surveillance Society?	Home Affairs Committee, House of Commons	BCS Response sent and publicly available	CLOSED
Electronic Patient Record and its use	House of Commons Select Committee	BCS Response sent and publicly available	CLOSED
Draft Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2007	Department of Constitutional Affairs	BCS response submitted	CLOSED
The removal of barriers to the sharing of non-consensual credit data	Department of Trade & Industry	BCS Response sent and publicly available	CLOSED
Online Availability Of Electronic Health Records	House of Commons Select Committee	BCS Response sent and publicly available	CLOSED
Electronic Voting	Intellect	BCS Letter of Intent supplied	CLOSED

InfoSec

Some of you may have visited InfoSec, Olympia in April. The BCS had a significant presence and the new stand design and layout meant it was sufficiently eye catching to draw quite a considerable footfall. There was a lot of interest in both general membership and specifically ISSG and IRMA membership and so I hope you will see increased membership and active contributions in the future. In particular, everyone seemed genuinely interested in their careers and the professionalism agenda - which are key tenets of the BCS message and mission. So this was good news. Thanks to those amongst you who helped to "person" the stand.

For me, attending InfoSec for the first time in a couple of years was an extremely rewarding and fruitful experience – an exhausting mixture of catching up on colleagues from years gone by; re-affirming links with present colleagues and industry experts and forging new relationships for future collaborations. It's certainly increased the "to do" list by a significant factor. But in all, ensuring that the BCS had a more prominent and professional presence at the show this year has so far reaped the appropriate rewards and we are looking forward to supporting the charter aims of the organisation for a very productive and hopefully secure (!) year ahead.

There was an excellent line up of speakers and topics – some of which were controversial!

But sadly, some of which were re-hashes of the same old stuff we've heard before. It was amazing to see people queuing in droves for all the different seminar options – particularly the Windows Vista Technical Programme talk and Bruce Schneier's Psychology of Security.

However, *question* – there were huge queues for the Hackers presentation at the end of the conference - how come it is still ok to support this kind of activity though? It really does make a mockery of the security

industry as being entirely self serving – i.e. we continue to maintain the "annonymity" of those who perpetrate crimes against those we seek to secure. It's a nonsense really – far too much theatre and not enough common sense.

One seminar in particular has sparked some ongoing interest and debate, rightly so! Derek Wyatt MP gave an extremely interesting talk about "Security and the Olympics" at which he put forward a number of scenarios that could amount to your job description/task list, should you be given what appeared to the "poison chalice" job of Information Security Director for the Games in 2012. Key to his meanderings was a description of how the UK, in spite of being responsible for the safety and well being of many thousands of visitors, would have to wait until the IOC and its chief sponsors (VISA in particular) dictated the technology that would be/should be used. This seemed preposterous to yours truly and I stood up and said so! We cannot allow yet another huge IT project to start off without building security in, rather than bolting it on at the end, when all the budget has been spent and proper time is not available. As professionals, we must co-ordinate and collaborate on this and ensure that the ODA is involving the right experts in the various relevant fields and that the MPs are in full understanding of the myriad of issues (i.e. in particular the level of likely technology threat, rather than just the obvious physical target threat). So the BCS is looking at hosting a one day seminar and get the ODA and interested parties to contribute, ahead of whatever advertising deals are done between the IOC and sponsors in a room talking about these issues. This story and the issues related has been picked up by ZDNet, ISN and BBC Online. Do get in touch of you are either a) involved or b) keen to be so!

In the meantime, if there are other burning issues that you passionately believe the BCS Security Forum should be involved in, please do get in touch so that we can ensure we seek support and collaboration as appropriate.

Andrea Simmons, CISSP, MBCS CITP, IISP, BA
Consultant Security Forum Manager BCS
Phone: 01905 356268
Mobile: 07961 508775
Email: andrea.simmons@bcs.org.uk
Web: www.bcs.org/security

The Devil's Guide to Spreadsheet Creation

Despite all the theory, this is how spreadsheets are really created according to the European Spreadsheet Users Interest Group (EuSprig)

1. Just do it. Jump in and do it. The users will have to accept whatever you produce anyway.
2. Fire, then aim. You know what is really needed without having to ask.
3. Never simplify (that just makes it easier for other people to get your job); just keep adding bits without removing old stuff.
4. Deadlines live on.
5. Documentation is for wimps; specifications are for the timid.
6. Don't obtain test data; whatever the spreadsheet result is, is right.
7. Don't protect the sheet; that restricts the users' right to improve your formulas by typing in what they want.
8. Don't fill in the properties sheet, they'll find out you were the author.
9. VBA (Very Buggy Application) debugging is easy; just keep making changes until something appears to work, then your responsibility is finished.
10. Never use in-cell comments or help text on the page; users should just know what to do.
11. If you know what units of measure are used, you can safely assume everybody else does too.
12. Mix input data with calculation cells to keep the users on their toes.
13. Never mix absolute and relative references, it can shorten billable time.
14. Hide some data in cells so that when users trip over it, their respect for your cleverness increases.
15. If asked to do a test run, ask "Don't you trust me?"
16. Format with as many decorative colours and styles as possible, to relieve boredom.
17. Don't keep backup copies of different versions of a spreadsheet, the latest is always the best.
18. Hardcode constants in formulas; after all, they don't change.
19. Cross-tot checking is merely redundant calculation.
20. To test a spreadsheet, you only need to check whether the answers look reasonable.

The consequences for falling for some or all of the above temptations are described in more than ninety spreadsheet problems at www.eusprig.org/stories.htm

SUGGESTED CHARTER FOR SYSTEM ADMINISTRATORS

Andrew Cormack

This document has been prepared by Andrew Cormack, Chief Regulatory Adviser at UKERNA. It is endorsed by the Universities and Colleges Information Systems Association (UCISA). Members of the UCISA Networking Group were closely consulted during the drafting process.

We hope that this charter will be useful to three groups: to users who wish to know the powers of administrators and to be assured that these will not be abused; to administrators themselves who are often concerned about the legality and implications of their actions; to managers to understand what are the reasonable requirements of the administrators' job and what activities they will be required to support.

Institutions will, of course, consult their legal advisers and make their own arrangements to comply with legislation. However, we suggest that this charter, or an equivalent statement of rights and responsibilities, should form part of the job description or job instructions of any person employed as a system or network administrator. We believe that this will go some way to compliance with the requirements for authorisation contained in the Regulation of Investigatory Powers Act 2000, and for procedures to protect personal data contained in the Data Protection Act 1998.

Acceptance of the rights and privileges of authorised administrators should be a condition of use of any computer connected to a network and also of connecting any computer to the network.

A Suggested Charter for System and Network Administrators

Version 1.3

Introduction

System and network administrators, as part of their daily work, need to perform actions which may result in the disclosure of information held by other users in their files, or sent by users over communications networks. This charter sets out the actions of this kind which authorised administrators may expect to perform on a routine basis, and the responsibilities which they bear to protect information belonging to others. Administrators also perform other activities, such as disabling machines or their network connections, that have no privacy implications; these are outside the scope of this charter and should be the subject of local working arrangements.

On occasion, administrators may need to take actions beyond those described in this charter. Some of these situations are noted in the charter itself. In all cases they must seek individual authorisation from the appropriate person in their organisation for the specific action they need to take. Such activities may well have legal implications for both the individual and the organisation, for example under the Data Protection and Human Rights Acts. Organisations should therefore ensure that they have information and procedures in place, including delegation of authority for routine requests, to ensure that such authorisation can be obtained promptly in all circumstances and is given in accordance with the law. Keeping good records, preferably against a pre-prepared checklist, will help to protect the investigator and the institution from any charge of improper actions.

System and network administrators must always be aware that the privileges they are granted place them in a position of considerable trust. Any breach of that trust, by misusing privileges or failing to maintain a high professional standard, not only makes their suitability for the system administration role doubtful, but is likely to be considered by their employers as gross misconduct. Administrators must always work within their organisation's information security and data protection policies, and should seek at all time to follow professional codes of behaviour such as the following:

- ACM Code of Ethics and Professional Conduct
- FEANI's Code of Conduct for Professional Engineers
- BCS Code of Conduct and Code of Good Practice
- SAGE Code of Ethics
- SANS IT Code of Ethics

Authorisation and Authority

System and network administrators require formal authorisation from the "owners" of any equipment they are responsible for. The law refers to "the person with a right to control the operation or the use of the system". In a university or college this right is likely to be delegated by the organisation to the Head of IT, or equivalent function. This person is therefore usually the appropriate authority to grant authorisation to network administrators working on the college network. Individual systems connected to the network may have more complicated ownership, as they may be formally the property of departments or other divisions. Authority in these cases will need to be worked out locally, but it may be easiest to delegate authority to the Head of IT either as part of the agreement by which a computer is managed centrally, or as a condition of connecting to the network. This document will use the term "Head of IT" on the assumption that authority over all systems on the network has been granted to that post: institutions may replace this be an appropriate title of group to suit local circumstances.

If any administrator is ever unsure about the authority they are working under then they should stop and seek advice immediately, as otherwise there is a risk that their actions may be in breach of the law.

Permitted Activities

The duties of system administrators can be divided into two areas.

The first duty of an administrator is to ensure that networks, systems and services are available to users and that information is processed and transferred correctly, preserving its integrity. Here the administrator is acting to protect the operation of the systems for which they are responsible. For example investigating a denial of service attack or a defaced web server is an operational activity as is the investigation of crime.

Many administrators also play a part in monitoring compliance with policies which apply to the systems. For example some organisations may prohibit the sending or viewing of particular types of material; or may restrict access to certain external sites, or ban certain services from local systems or networks. The JANET Acceptable Use Policy prohibits certain uses of the network. In all of these cases the administrator is acting in support of policies, rather than protecting the operation of the system.

The law differentiates between operational and policy actions, for example in section 3(3) of the *Regulation of Investigatory Powers Act 2000*, so the administrator should be clear, before undertaking any action, whether it is required as part of their operational or policy role. The two types of activity are dealt with separately in the following sections.

Operational activities

Where necessary to ensure the proper operation of networks or computer systems for which they are responsible, authorised administrators may:

- monitor and record traffic on those networks or display it in an appropriate form;
- examine any relevant files on those computers;
- rename any relevant files on those computers or change their access permissions (see Modification of Data below);
- create relevant new files on those computers.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it, the administrator must not attempt to make the content readable without specific authorisation from the Head of IT or the owner of the file.

The administrator must ensure that these activities do not result in the loss or destruction of information. If a change is made to user filestore then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

Policy activities

Administrators must not act to monitor or enforce policy unless they are sure that all reasonable efforts have been made to inform users both that such monitoring will be carried out and the policies to which it will apply. If this has not been done through a general notice to all users then before a file is examined, or a network communication monitored, individual permission must be obtained from all the owner(s) of files or all the parties involved in a network communication.

Provided administrators are satisfied that either a general notice has been given or specific permission granted, they may act as follows to support or enforce policy on computers and networks for which they are responsible:

- monitor and record traffic on those networks or display it in an appropriate form;
- examine any relevant files on those computers;
- rename any relevant files on those computers or change their access permissions or ownership (see Modification of Data below);
- create relevant new files on those computers.

Where the content of a file or communication appears to have been deliberately protected by the owner, for example by encrypting it or by marking it as personal, the administrator must not examine or attempt to make the content readable without specific authorisation from the Head of IT or the owner of the file.

The administrator must ensure that these activities do not result in the loss or destruction of information. If a change is made to user filestore then the affected user(s) must be informed of the change and the reason for it as soon as possible after the event.

Disclosure of information

System and network administrators are required to respect the secrecy of files and correspondence.

During the course of their activities, administrators are likely to become aware of information which is held by, or concerns, other users. Any information obtained must be treated as confidential - it must neither be acted upon, nor disclosed to any other person unless this is required as part of a specific investigation:

- Information relating to the current investigation may be passed to managers or others involved in the investigation;
- Information that does not relate to the current investigation must only be disclosed if it is thought to indicate an operational problem, or a breach of local policy or the law, and then only to the Head of IT (or, if this is not appropriate, to a senior manager of the organisation) for them to decide whether further investigation is necessary.

Administrators must be aware of the need to protect the privacy of personal data and sensitive personal data (within the meaning of the Data Protection Act 1998) that is stored on their systems. Such data may become known to authorised administrators during the course of their investigations. Particularly where this affects sensitive personal data, any unexpected disclosure should be reported to the relevant data controller.

Intentional Modification of Data

For both operational and policy reasons, it may be necessary for administrators to make changes to user files on computers for which they are responsible. Wherever possible this should be done in such a way that the information in the files is preserved:

- rename or move files, if necessary to a secure off-line archive, rather than deleting them;
- instead of editing a file, move it to a different location and create a new file in its place;
- remove information from public view by changing permissions (and if necessary ownership).

Where possible the permission of the owner of the file should be obtained before any change is made, but there may

be urgent situations where this is not possible. In every case the user must be informed as soon as possible what change has been made and the reason for it.

The administrator may not, without specific individual authorisation from the appropriate authority, modify the contents of any file in such a way as to damage or destroy information.

Unintentional Modification of Data

Administrators must be aware of the unintended changes that their activities will make to systems and files. For example, listing the contents of a directory may well change the last accessed time of the directory and all the files it contains; other activities may well generate records in logfiles. This may destroy or at best confuse evidence that may be needed later in the investigation.

Where an investigation may result in disciplinary charges or legal action, great care must be taken to limit such unintended modifications as far as possible and to account for them. In such cases a detailed record should be kept of every command typed and action taken. If a case is likely to result in legal or disciplinary action, the evidence should first be preserved using accepted forensic techniques and any investigation performed on a second copy of this evidence.

References

It is not possible to list all the legislation which applies to the work of system and network administrators. However the following Acts are particularly relevant to the activities covered by this charter.

- *The Regulation of Investigatory Powers Act 2000* and the secondary *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*;
- The *Data Protection Act 1998*;
- The *Human Rights Act 1998*.

The Office of the Information Commissioner's Employment Practice Code (with quick guide and supplementary guidance) includes a section on Monitoring at Work, including use of computers and networks.

Guidelines to good forensic practice are available, for example

- Association of Chief Police Officers (ACPO) Good Practice Guide for Computer Based Evidence;
- JISCLegal technical investigation process;
- CERT Co-ordination Center First Responders Guide to Computer Forensics (USA)

A selection of examples have been written to illustrate how the charter might be applied to particular situations.

Picture this – your secrets lost before your very eyes

Alan Woodward

Alan Woodward of Charteris says a picture may be worth a thousand words, but it could also hide something more treacherous.

Today, businesses wanting to guard against the potentially ultra-serious hazard of vitally important data being deliberately leaked to unauthorised people outside or even inside the organisation, need to get to grips with an alarming reality: a picture can also conceal a thousand words.

Or in some cases even up to around 5,000 words. More than enough to betray all your most precious and commercially sensitive data: locations of newly-discovered oil fields; formulae for synthesising newly-discovered molecules of breakthrough drugs costing millions or even billions to develop; designs of revolutionary products you're planning on being the first to bring to market; ultra-sensitive lists of hard-won customers; you name it.

Data concealed in pictures? It may sound like the basis for a plot sequence in the next Mission Impossible movie, but it isn't. It's real. And unless you are prepared to let any Tom, Dick or Harry cruise around your precious data, you need to be aware of the threat it poses.

The technique is called steganography, from Ancient Greek words meaning hidden or covered writing, just as that lumbering dinosaur the stegosaurus is so named because its back was covered in those large bony plates whose real purpose is a mystery even today.

But steganography wasn't a mystery to the Ancient Greeks; indeed they most likely invented it. The Greek historian Herodotus records that in 312 BC, Histaeus of Miletus commanded the head of his most trusted slave to be shaved and tattooed with a vitally important secret message on it. Once the slave's hair had grown, hiding the message, Histaeus used him as an emissary to a friendly power via enemy territory to instigate a revolt against the Persians.

This example from history shows why steganographic writing is such a dangerous threat to security. Friends who betray us are always a more potent threat than people we recognise as enemies from the outset, and steganographic messages look friendly and innocent.

You could devise a simple steganographic message by agreeing with your recipient that your real message will consist of the first letter of every word of your apparent message. 'Bring us your invoice by Monday', for example, would really mean 'BUY IBM'. In steganographic writing the apparent message is known as the covertext and the real message is called the plaintext.

The innocuous appearance of the covertext in the example illustrates why steganographic writing doesn't tend to set alarm bells ringing. It looks innocent, whereas the message 'BUY IBM' encrypted in a simple code that consisted, say, of substituting each letter for the next letter in the alphabet - 'CVZ JCN' - obviously looks dodgy and would be certain to awaken the suspicions of even the most credulous member of an industrial espionage prevention team.

The point is that any encrypted message will tend to raise suspicions because even though it can't readily be read you will know it's been encrypted and will instantly conclude that something fishy's going on.

In the highly competitive ocean of modern business, the threat of steganography has recently become a major issue in corporate life.

It's actually been a significant threat for several years due to the increased computing power available on everyone's desktop, but people have been distracted by publicity about cryptography and steganography has rather remained in the background.

It's a particularly worrying threat now because of the enormous computing power on desktops today, the massive volume of electronic communications, and the number of freely available tools that allow even a routine user to employ steganographic techniques.

By far the biggest type of threat is the potential for concealing steganographic writing within computerised images. With Windows you can literally drag and drop your hidden text onto a picture and the deed is done.

As Gordon Gekko reminded us in the film Wall Street (1985), the most valuable commodity of all is information. And it's precisely that which can so easily be given away today - or sold - using image-based steganographic techniques.

What's actually happening when you carry out what looks like a simple drag and drop?

An electronic image is comprised of thousands of 'picture elements' or 'pixels'. A pixel is a binary number that provides information on the colour or (in a black and white picture) the shade of grey that should be displayed in that particular pixel.

The binary number will look something like this: 10011011 etc depending on the pixel in question. The individual numbers (the 1 or the 0) are known as bits and the further along you go to the right the less significant the bits become in defining the precise colour of the pixel.

Why does the opportunity for steganography exist? Because while each pixel is defined by a series of bits, some of these bits can be changed without affecting the resulting pixel to any discernible extent. In a computerised image whose size is 256 by 256 pixels, making a total of 65,536 pixels, there would easily be room to conceal say, about 5,000 words of data.

This method of concealment is known as 'bit twiddling'. An obvious place to conceal a secret message would be within a computerised picture that does not show any apparent changes.

Bit twiddling is the most common way to conceal text within a computerised image. There are many more techniques,

though, particularly when using image formats such as the now ubiquitous jpeg which many will have encountered through their digital cameras.

An apparently innocuous picture of - of example - an employee's child's first day at school taken with a standard family digital camera could easily be used to conceal a damaging leak. The leak could be so fatal that by the time the school term ends, thousands of other mums and dads at the business from which the information was leaked will have had to find new jobs - if they can.

What's the best way to guard against the hazard of modern image-based steganographic betrayal?

The first step is to recognise that it is a potential problem and get help to understand what tools are likely to be available to a malicious team member. You also need to know the manner in which these tools can be used because they often leave little trace of their presence - some are even termed 'zero footprint' by those who develop them.

Yet help is at hand because dedicated teams of experts have been making available tools to help detect steganography. The technique they use is known as 'steganalysis'.

Steganalysis is as much an art as a science. The detection tools need to be used so that the appropriate steganalysis resource is used in the appropriate situation.

Admittedly, this is not easy, when the range of steganography tools and the steganalysis counterparts have proliferated and are proliferating just as the threat from viruses did when they first emerged into the IT environment.

At Charteris we began our own anti-steganography work as a technical exercise but were soon alarmed at what our experiments were telling us, not just about the power of the steganography tools available but also about the degree of care that needs to be applied to combat this potent security hazard.

Taking the threat of betrayal by apparently innocuous pixels seriously will lead you to put into practice the measures necessary to defend against it. And you do need to take this threat very seriously indeed. The stegosaurus may be long extinct, but steganographic treachery is, unfortunately, here to stay.

Alan Woodward is chief technology officer at the business and information technology consultancy Charteris.

Alan Woodward, Executive Director
Charteris plc, Charteris House,
39-40 Bartholomew Close,
London EC1A 7JN

Switchboard: +44 (0)20 7600 9199
Mobile: +44 (0)7887 745 270
Fax: +44 (0)20 7600 9212
alan.woodward@charteris.com

Recruitment Advice

- Put 400 bricks in a closed room.
- Put your potential recruits in the room and close the door.
- Leave them alone and come back after 8 hours.
- Then analyze the situation:
    - If they are counting the bricks, put them in the Accounting Department.
    - If they are recounting them, put them in Audit.
    - If they have messed up the whole place with the bricks, put them in Engineering.
    - If they are arranging the bricks in some strange order, put them in Planning.
    - If they are throwing the bricks at each other, put them in Operations.
    - If they are sleeping, put them in Security.
    - If they have broken the bricks into pieces, put them in Information Technology.
    - If they are sitting idle, put them in Human Resources.
    - If they say they have tried different combinations, they are looking for more, yet not a brick has been moved, put them in Sales.
    - If they have already left for the day, put them in Marketing.
    - If they are staring out of the window, put them in Strategic Planning.
    - If they are talking to each other, and not a single brick has been moved, congratulate them and put them in Top Management.
    - If they have surrounded themselves with bricks in such a way that they can neither be seen nor heard from, put them in Parliament.

HUMOUR PAGES

Support Desk Woes

Tech Support: *"I need you to right-click on the Open Desktop".*
Customer: *"OK".*
Tech Support: *"Did you get a pop-up menu?".*
Customer: *"No".*
Tech Support: *"OK. Right-Click again. Do you see a pop-up menu?"*
Customer: *"No".*
Tech Support: *"OK, sir. Can you tell me what you have done up until this point?".*
Customer: *"Sure. You told me to write 'click' and I wrote 'click'".*

Tech Support: *"OK. In the bottom left hand side of the screen, can you see the 'OK' button displayed?"*
Customer: *"Wow. How can you see my screen from there?"*

Caller: *"I deleted a file from my PC last week and I have just realised that I need it. If I turn my system clock back two weeks will I have my file back again?".*

...to make a life a little bit easier!

Old telephone books make ideal personal address books. Simply cross out the names and addresses of people you don't know.

Fool other drivers into thinking you have an expensive car phone by holding an old TV or video remote control up to your ear and occasionally swerving across the road and mounting the curb.

Avoid parking tickets by leaving your windshield wipers turned to fast wipe whenever you leave your car parked illegally.

No time for a bath? Wrap yourself in masking tape and remove the dirt by simply peeling it off.

Save on booze by drinking cold tea instead of whiskey. The following morning you can create the effects of hangover by drinking a thimble full of dish washing liquid and banging your head repeatedly on the wall.

If a person is choking on an ice cube, don't panic. Simply pour a jug of boiling water down their throat and presto! The blockage is almost instantly removed.

Apply red nail polish to your nails before clipping them. The red nails will be much easier to spot on your bathroom carpet. (Unless you have a red carpet, in which case a contrasting polish should be selected).

Colour-coordinate your pet with your furniture and carpets. That way, the hair won't show if you don't regularly sweep it up.

When Insults Had Class

"He has all the virtues I dislike and none of the vices I admire."
— Winston Churchill

"A modest little person, with much to be modest about."
— Winston Churchill

"I have never killed a man, but I have read many obituaries with great pleasure."
— Clarence Darrow

"He has never been known to use a word that might send a reader to the dictionary."
— William Faulkner (about Ernest Hemingway)

"Poor Faulkner. Does he really think big emotions come from big words?"
— Ernest Hemingway (about William Faulkner)

"Thank you for sending me a copy of your book; I'll waste no time reading it."
— Moses Hadas

"He can compress the most words into the smallest idea of any man I know."
— Abraham Lincoln

"I've had a perfectly wonderful evening. But this wasn't it."
— Groucho Marx

"I didn't attend the funeral, but I sent a nice letter saying I approved of it."
— Mark Twain

"He has no enemies, but is intensely disliked by his friends."
— Oscar Wilde

"I am enclosing two tickets to the first night of my new play; bring a friend ... if you have one."
— George Bernard Shaw to Winston Churchill

"Cannot possibly attend first night, will attend second ... if there is one."
— Winston Churchill, in response

"I feel so miserable without you; it's almost like having you here."
— Stephen Bishop

"He is a self-made man and worships his creator."
— John Bright

"I've just learned about his illness. Let's hope it's nothing trivial."
— Irvin S. Cobb

"He is not only dull himself, he is the cause of dullness in others."
— Samuel Johnson

"He is simply a shiver looking for a spine to run up."
— Paul Keating

"He had delusions of adequacy."
— Walter Kerr

"There's nothing wrong with you that reincarnation won't cure."
— Jack E. Leonard

"He has the attention span of a lightning bolt."
— Robert Redford

"They never open their mouths without subtracting from the sum of human knowledge."
— Thomas Brackett Reed

"He inherited some good instincts from his Quaker forebears, but by diligent hard work, he overcame them."
— James Reston (about Richard Nixon)

"In order to avoid being called a flirt, she always yielded easily."
— Charles, Count Talleyrand

"He loves nature in spite of what it did to him."
— Forrest Tucker

"Why do you sit there looking like an envelope without any address on it?"
— Mark Twain

"His mother should have thrown him away and kept the stork."
— Mae West

"Some cause happiness wherever they go; others, whenever they go."
— Oscar Wilde

"He uses statistics as a drunken man uses lamp-posts ... for support rather than illumination."
— Andrew Lang (1844-1912)

"He has Van Gogh's ear for music."
— Billy Wilder

……. and my favourite, as it relates wonderfully well to an IS auditor ……..

"Success is not final .. failure is not fatal .. it is the courage to continue that counts".
— Winston S Churchill

Actual letter of resignation from an employee at Fortex Computers, USA, to her boss, who apparently resigned very soon afterwards!

Dear Mr. Baker,

As a graduate of an institution of higher education, I have a few very basic expectations. Chief among these is that my direct superiors have an intellect that ranges above the common ground squirrel. After your consistent and annoying harassment of my co-workers and me during the commission of our duties, I can only surmise that you are one of the few true genetic wastes of our time.

Asking me, a network administrator, to explain every little nuance of everything I do each time you happen to stroll into my office is not only a waste of time, but also a waste of precious oxygen. I was hired because I know how to network computer systems, and you were apparently hired to provide amusement to myself and other employees, who watch you vainly attempt to understand the concept of "cut and paste" for the hundredth time.

You will never understand computers. Something as incredibly simple as binary still gives you too many options. You will also never understand why people hate you, but I am going to try and explain it to you, even though I am sure this will be just as effective as telling you what an IP is. Your shiny new iMac has more personality than you ever will. You walk around the building all day, shiftless looking for fault in others. You have a sharp dressed useless look about you that may have worked for your interview, but now that you actually have responsibility, you pawn it off on overworked staff, hoping their talent will cover for your glaring ineptitude. In a world of managerial evolution, you are the blue-green algae that everyone else eats and laughs at. Managers like you are a sad proof of the Dilbert principle. Since this situation is unlikely to change without you getting a full frontal lobotomy reversal, I am forced to tender my resignation, however I have a few parting thoughts.

1. When someone calls you in reference to employment, it is illegal for you to give me a bad recommendation. The most you can say to hurt me is "I prefer not to comment." I will have friends randomly call you over the next couple of years to keep you honest, because I know you would be unable to do it on your own.

2. I have all the passwords to every account on the system, and I know every password you have used for the last five years. If you decide to get cute, I am going to publish your "favourites list", which I conveniently saved when you made me "back up" your useless files. I do believe that terms like "Lolita" are not usually viewed favourably by the administration.

3. When you borrowed the digital camera to "take pictures of your Mother's birthday," you neglected to mention that you were going to take pictures of yourself in the mirror nude. Then you forgot to erase them like the techno-moron you really are. Suffice it to say I havenever seen such odd acts with a sauce bottle, but I assure you that those have been copied and kept in safe places pending the authoring of a glowing letter of recommendation. (Try to use a spell check please; I hate having to correct your mistakes).

Thank you for your time, and I expect the letter of recommendation on my desk by 8:00 am tomorrow. One word of this to anybody, and all of your little twisted repugnant obsessions will be open to the public. Never muck with your systems administrator. Why? Because they know what you do with all that free time!

Wishing you a grand and glorious day,

Michelle

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

BCS
THE BRITISH COMPUTER SOCIETY

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 *(NOT a member of the BCS)* For details of BCS membership visit www.bcs.org	£25
INDIVIDUAL MEMBERSHIP *(A members of the BCS)* BCS membership number: _____	FREE
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).* Educational Establishment: _____	FREE

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 — 4 = Academic 2 = External Audit — 5 = Full-Time Student 3 = Data Processor — 6 = Other (please specify)
SIGNATURE: DATE:

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

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

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