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

JOURNAL
volume 16 number 4 winter 2006 ISSN 1741-4229

BCS
THE BRITISH COMPUTER SOCIETY

Programme of Briefings & Meetings 2007

Title	Meeting type	Date
Hacking using search engines (speaker Peter Wood)	Late Afternoon	Tuesday 6 February 2007
Event TBA	Late Afternoon	Tuesday 6 March 2007
Event TBA	Late Afternoon	Tuesday 3 April 2007
AGM and twilight Event TBA	Late Afternoon	Tuesday 1 May 2007
Mobile Devices and Network Security (Stan Dormer)	Late Afternoon	Tuesday 5 June 2007

Apart from any joint meetings with other organizations all meetings will be held at BCS, 5 Southampton Place, London WC2
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 with your membership renewal or to the chair at brewer.alex@gmail.com (preferably with the subject "IRMA contact details"). 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
Email: john@lhscontrol.com

Produced by Carliam Artwork, Potters Bar, Herts

Editorial

John Mitchell

"They that can give up essential liberty to purchase a little temporary safety deserve neither liberty or safety."
– Benjamin Franklin

Some months ago, Alex Brewer the then Chairman of this group, pointed out that the new British passports contained a wi-fi transponder which had not been widely mentioned in all the ho-hah relating to the proposed bio-metric passports. Indeed, the roll out of this relatively undocumented feature had already commenced and his daughter's passport was so enabled. The Government stated that the encryption used was triple DES and no-one need concern themselves about passport identity theft by someone interrogating the chip. Now the basic rule of encryption is that you assume that the other side will know the process, but hope that they do not know the key that you are using. However, with these passports the key is actually displayed in the printed part of the passport itself. It comprises the passport number, the holder's date of birth and the passport expiry date. All of which, as reported by the Guardian[1] newspaper, are often required at hotel registration desks to get a room. If you couple that information with an RFID scanner (£174 at your favourite electrical store) you can suck out all the biometric information from the chip and create your own perfect clone. I accept that you still need to forge the actual passport, but it probably does not need to be a perfect copy as the immigration authorities will most likely rely on the data in the chip. If fingerprint recognition is used, then you can use the data in the chip to create the matching set on silicone which then fit snugly over your real prints. The Home Office claim that you have to be really close to the chip to interrogate it, but the Guardian researcher was able to do so from a distance of ten metres which included a couple of walls in the way too.

A few years ago I predicted that with the roll out of RFID chips in the retail sector the criminals of the future would only have to scan you, your car, or your house to decide if you were worth robbing. I was laughed at by the consultants selling the technology on two grounds. First, all chips would be disabled once the product left the store and second the distance thing already mentioned. I did not believe at the time that the first would happen and even if it was so intended it would not be perfect and I had no faith at all in the distance argument as advances in technology would enable that to be solved. My advice is to use disinformation. Obtain a load of RFID chips that identify your clothes as being from ASDA and not Amarni, your watch as a Timex rather than a Rolex and showing your ring as containing zircon and not diamond. Go one stage further and carry with you another chip containing passport information belonging to someone else (preferably someone well known for their martial arts skills) to give the muggers something to think about when they "read you". Here is another prediction, the term "to read you" will enter the English vocabulary in much the same as "to Google" already has, but with far more serious undertones.

As someone once said, if you want to eat an elephant do it one small piece at a time as otherwise you will get acute indigestion. What they don't say is which piece you should eat first? Providing assurance on IT can be like eating an elephant, but at least we have a guide as to where we should start. General controls first, followed by the specifics. As the applications rely on the infrastructure and the infrastructure comprises the hardware, base software and network stuff, then it's pretty obvious that an accurate asset register is the starting point. If they haven't got that, then how can the CIO know that things are well controlled? IT comprises around 34 key processes with all the associated interactions. If we can measure the absolute maturity of each process and its relative importance to the other processes, then we have a further indication as to where we should target our resources. We have great toolkits available to us ranging from CobiT[2] through ISO 27001, ISO 20001, ITIL and ISO 9126 to name but a few. We also have associated qualifications such as CISA[3] and CISM[4] which indicate our professional attainments. Put this heady mix together and

[1] 17th November 2006
[2] Control Objectives for IT from the Information Systems Audit & Control Association
[3] Certified Information Systems Auditor
[4] Certified Information Security Manager

we become pretty much invincible in justifying the work that we do and the assurance that we can provide. Co-active auditing as I call it (working with the clients rather than against them) does not mean us lying down with our legs in the air, but it does require a degree of confidence that I often see sadly lacking in many IT auditors. Forget about friendship, it's respect that we crave. To get that you also have to have it for the other side. Mutually assured respect (MAS) is something we need to work on. They need to as well.

In this edition Bruce (Harv) Busta, Kris Portz, Joel Strong & Roger Lewis bring us the results of their research into the most important controls for small businesses. Ryan Purita educates us on computer forensics, while Bob Ashton draws our attention to the worlds of virtual crime. Jean Morgan reports on our financial situation and Mark Smith has provided his usual helpful list of members' benefits which shows the value for money you receive from your membership subscription. Lou Agosta deals with the thorny subject of governing data governance and Davis Clarke our parent body's CEO covers the need for professionalism. Which is where I ended up in my editorial.

The compliments of the season to you all and I hope to see you at our next meeting in the New year.

Don't forget to volunteer for your Management Committee. We are really desperate to persuade someone to help us with membership.

IRMA MEMBERS' BENEFITS DISCOUNTS

Mark Smith

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)

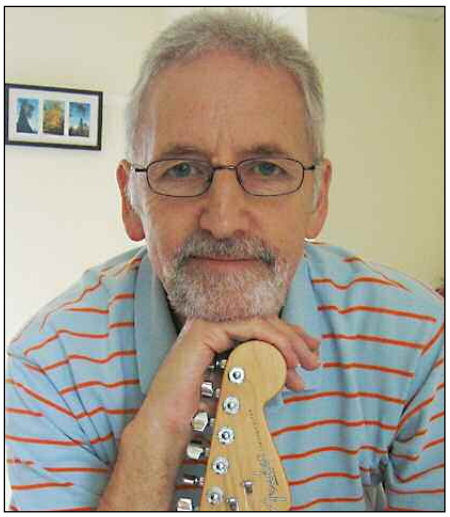
Events

Event	Discount Negotiated	Contact
E-Tec courses (www.e-tecsecurity.com)	10%	Margaret Mason (info@e-tecsecurity.com)
IACON 2006 (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)
Websec 2006 (www.mistieurope.com)	15%	Lisa Davies (LDavies@mistiemea.com)

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



"So long, and thanks for all the fish/phish/fiche…"

In the Spring of 2003, my pal Alex Brewer took over the mantle of Chairman of the IRMA management committee from the previous incumbent, John Bevan. Sadly, personal circumstances (see Autumn 2006 Journal) have recently dictated that after just 3 years, he is resigning the post and committee membership, but not before stamping his own style of delivery with enthusiasm and humour on to IRMA proceedings.

Alex introduced electronic mind-mapping to the committee, obviating the need for us to make copious meeting notes, and he set up "Pipeline" – a spreadsheet method of planning, owning and preparing for IRMA events. In "sleeves-rolled-up" mode, he has taken more than his fair share of presentations at evening sessions (plus some last minute sessions at day events) and his knowledge of Wi-Fi and wariness of the invasive nature of RFID technology are now legendary within the group.

Then again, someone who plays acoustic guitar like he does can't be all bad…

Also a word about Raghu Iyer, a long-standing committee member who has also decided to hang up his IRMA boots. In my time as a committee member (since 2003), he radically redesigned the event-planning process to ensure that presentations actually happened in a well-structured manner, with only the most gentlemanly form of harassment towards speakers/organisers to get their act in order so that it would be alright on the night.

Raghu could also be relied upon to turn any committee crisis into a laughing matter, thus taking the sting out of adverse situations and motivating the troops to a satisfactory outcome.

So, I hope Alex and Raghu are reading this and will accept the grateful thanks of IRMA for their sterling contributions and best wishes for the future. We hope to see them at IRMA events, perhaps providing a filler for that embarrassing silence that often follows the phrase "Thank you very much for an enlightening presentation. Does anyone have any questions?"

Thanks also are due to Jean Morgan for temporarily but bravely stepping into the breach as Chair and Treasurer – probably a conflict of interests there, but when needs must, pragmatism has to prevail!

Hello, there …

So here am I, having adopted the Chairman's (virtual) chain of office until the next AGM.

What can I say about Ross John Palmer, MIIA, FIIA, CISA, FBCS CITP, Guitar (Grade 8) and Cycling Proficiency (with Hons)?

I thought that the best way of introducing myself to the readership is to relate my dislikes, which are always more compelling. I am unlikely to be famous enough to appear on "Room 101" or "Grumpy Old Men", but here are a couple of illustrative grouses of mine:

- Getting stuck behind a slow-moving horse box on a narrow, winding country road. Solution –use bubble-wrap round the horses' girth to protect it then put the foot down a bit.
- The UK National Anthem – I go with the excellent sentiments, but the music is a bit of a dirge. Wouldn't it be good to see the Union Flag rising at the Olympics to the up-tempo "Thunderbirds" theme, or similar?

To which I can add the technology-related:

- My handwriting, which has deteriorated so much and probably irretrievably, since using a PC keyboard. However, I try to maintain standards of spelling and grammar in my emails and texts despite the curious "which/that" grammar checks or the particularly unhelpful "fragment (consider revising)".
- Email – why provide a read receipt function when the recipient can opt to withhold it?
- Upgraded versions of software that add little but costs and re-training. Learning new ways of doing things that one only just got to grips with must cost industry dearly.

In the news …

- YouGov has published a survey giving an interesting slant on UK brand-awareness. What would you think are the UK public's favourite consumer brands in 2006? HP Sauce? Rolls-Royce? Marks and Spencer? No, it's Microsoft, who beat the BBC and British Airways to the number one slot.
- PayPal and eBay are now the biggest targets of phishing attacks, together accounting for more than 75% of phishing emails, according to research by Sophos, who gave the reason that PayPal and eBay now have more of a global identity than individual banks.

- RSA Security's annual password management survey has determined that the high volume of business passwords is overwhelming users and undermining IT security. Almost a fifth of respondents said they had more than 15 passwords, although just five per cent said they could remember that many. An adjunct to this comes from Securetest who, in their laptop security presentation to IRMA (3 October), said that, as most hacking tools are developed in and deployed from the USA, where the "£" and "€" symbols do not appear on keyboards by default, these are good characters to use in UK passwords as a defence against brute-force password crackers.

- Technological innovation is now bringing us a laptop video projector the size of a sugar cube, screens for use with laptops that can be rolled up and put into a pocket and the ubiquitous RFID tags being embedded into airline boarding passes which, apparently, in combination with CCTV cameras, can find passengers at airports who do not respond to last boarding calls.

- As I write these words, the first ever Internet Governance Forum, set up by the United Nations, is taking place in Athens. The idea is to bring global internet stakeholders together in one place and reach agreement on internet-related issues, such as cybercrime, security, spam, etc. Opposing views are aired on sensitive subjects, such as freedom of speech, and while agreement may be reached for solutions, there are pessimistic views on how they can be enforced. Still, agreement on the problems seems to be a good place to start.

BCS Security Website

The new BCS Security website (www.bcs.org/security) is an excellent source of information for those with an interest in all aspects of IT security and I can thoroughly recommend it.

And finally… risk management comes to life !

A personal experience brought risk management well to the fore recently when, sitting at my desk one morning, I felt something crawling up my leg inside my trousers that probably should not have been there. A very hasty transition to the washroom, which must have left colleagues wondering about my state of gastric health, resulted in me shaking out on to the floor … a wasp! It must have been there since I pulled on my trousers that morning, being happy to be driven to work, and was obviously – and luckily – too sleepy or inebriated (on the rotting windfall apples in our garden) to use its business end on my person. I determined that the best preventive control over this would be cycle clips while another colleague suggested transferring the risk … by stuffing the wasp up someone else's trouser leg !

Until the next time, if you would like to get in touch, suggest topics for coverage, even join the committee (wishful thinking on my part? I hope not), then please use the email address **chair.irma@bcs.org.uk**

Meanwhile, take care and have a Happy Christmas (which means the Easter Eggs will soon be in the shops).

LETTER TO THE EDITOR

Dear Editor,

I am quite sure my IRMA membership subscription doesn't cover the value I receive from the briefings, seminars and Journal. The balance of the value derived by members comes from a generous contribution of personal effort and inspiration by the editorial panel, management committee and supporters. This is one opportunity to express appreciation for the effort of which members are, I am sure, aware but don't always find a chance to articulate.

Has there been an increased trend towards publishing technical articles recently? This aspirational development is a great opportunity to make a statement about IRMA and its members and I wish it every success. This is not to suggest the Journal content is out of balance - I always enjoy the humour pages and the programme and general content are always useful.

Hopefully, IRMA will survive and thrive so that we, the members, may continue to enjoy such excellent value-for-money from a modest professional subscription.

Regards
Tony Mullany

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

Virtual Crime Worlds

Two new technology based products have recently been identified which can be, and no doubt will be, used to facilitate identity theft, money laundering, and other crime.

Spoofcard - "Be who you want to be"

Most people are familiar with telephone calling cards – for a pre paid charge one can purchase an amount of "talk time", without the need to have a fixed phone or a contract with a phone company. An enhanced version of this product is being marketed in North America which is specifically designed to conceal or falsify the identity of the caller.

Unique Features

Spoofcard.com is marketing a product, currently only available in the US and Canada, which carries some disturbing implications.

Spoofcard.com sells calling cards through the internet for as little as $10 for 60 minutes talk time. The service provides a toll free number where the user enters a PIN, any caller ID telephone number they choose, and the number they wish to call. When the call connects, if the recipient has caller ID enabled, the false ID is shown, or if the spoofed caller ID telephone number is listed in the public telephone directory, a reverse telephone directory database is accessed and a spoofed identity corresponding to the false caller ID telephone number is displayed.

The final refinement of the system is its ability to create an altered voice. The user has the ability to select a male or female voice when making a call. Although the caller speaks normally the recipient hears the altered voice. Computer processing changes the caller's voice in real time.

Claimed Legitimate Uses

Spoofcard states that its target market consists of, but is not limited to, businesses such as: Private Investigators, Law Enforcement, Skip Tracers, Insurance Agencies and Lawyers.

The advantages claimed for Caller ID spoofing are:

- ✔ Caller ID spoofing gives business professionals the ability to manipulate their identity to one of their choosing and stay anonymous.
- ✔ Caller ID spoofing is valuable in defeating popular telephone services such as "*57 Call Trace", "69 Last Call Return", "Anonymous Call Rejection" and "Detailed Billing".
- ✔ Private Investigators will find Caller ID spoofing valuable for pretext[1] calls.

[1] *Pretext is a term used to illegally obtain information, such as telephone or bank records by pretending to be the owner of the account. The term comes from the fact that the caller uses a pretext along the lines "I just need to check when that number was dialled", etc.*

Criminal Uses

Spoofing gives criminals the ability to hide the calling number, manipulate their identity and stay anonymous. This will prevent detailed billing, anonymous call rejection and could mislead law enforcement agencies with regard to telephone intercepts, call charge records and reverse call charge records. It will also be easier for identity thieves to collect personal details of recipients by impersonating officials of churches, financial institutions etc., leading to all sorts of identity fraud.

Second Life – "Your World Your Imagination"

Second Life as the Metaverse

"Second Life is one of several virtual worlds that have been inspired by the science fiction novel *Snow Crash* by Neal Stephenson, and the Cyberpunk literary movement . The stated goal of its creators, Linden Lab, is to create a world like the metaverse described in the novel *Snow Crash*, a user-defined world of general use in which people can interact, play, do business, and otherwise communicate. Despite its prominence, it has notable competitors, among them Active Worlds, considered by many to be the founding company of the 3D internet concept in 1997, There and newcomers such as Entropia Universe and the Dotsoul Cyberpark, which is rapidly gaining recognition around the cybersphere as a metaverse aspirant with an emphasis on noncommercial culture." - Wikipedia

As unlikely as it may seem, Kevin Zucato, the director of the Australian High Tech Crime Centre (AHTCC) has warned that

such on-line worlds, created for entertainment purposes, had the potential to become terrorist hotbeds enabling untraceable communications, transfer of funds and money laundering.

Inhabitants of Second Life spend Linden dollars ($L), named after a street in San Fransisco, and purchased at an on-line currency exchange, buying anything that a person in the real world would spend cash on. Mr. Zucato said that problems could arise in the open environment, with globally dispersed, anonymous users. On-line communities removed the basic tools of law enforcement, such as the ability to observe someone acting suspiciously, follow them and search their property. Most internet service providers would store information only for a maximum of 90 days, which means that unless someone was under specific surveillance evidence of their communications and financial dealings would soon evaporate. He is concerned that the economy of virtual worlds could act as a front for real world crime. Without careful scrutiny money laundering and large fund transfers could pass under the radar.

"If I was a terrorist and I wanted to conspire to blow something up in Australia, I would get my associates in different countries to log on to Second Life, go to one of the coffee shops and discuss our plot using text or voice over IP."

For further information:

www.spoofcard.com
www.secondlife.com

LAWS OF THE NATURAL UNIVERSE

Law of Mechanical Repair: After your hands become coated with grease, your nose will begin to itch or you'll have to pee.

Law of the Workshop: Any tool, when dropped, will roll to the least accessible corner.

Law of Probability: The probability of being watched is directly proportional to the stupidity of your act.

Law of the Telephone: If you dial a wrong number, you never get a busy signal.

Law of the Alibi: If you tell the boss you were late for work because you had a flat tyre, the very next morning you will have a flat tyre.

Variation Law: If you change traffic lanes, the one you were in will start to move faster than the one you are in now (works every time).

Law of the Bath: When the body is fully immersed in water, the telephone rings.

Law of Close Encounters: The probability of meeting someone you know increases when you are with someone you don't want to be seen with

Law of the Result: When you try to prove to someone that a computer (or any other device) won't work, it will.

Law of Biomechanics: The severity of the itch is inversely proportional to the reach.

Law of the Theatre: At any event, the people whose seats are furthest from the aisle arrive last.

Law of Coffee: As soon as you sit down to a cup of hot coffee, your boss will ask you to do something which will last until the coffee is cold.

Murphy's Law of Lockers: If there are only two people in a locker room, they will have adjacent lockers.

Law of Rugs/Carpets: The chances of an open-faced jam sandwich landing face down on a floor covering are directly correlated to the newness and cost of the carpet/rug.

Law of Location: No matter where you go, there you are.

Law of Logical Argument: Anything is possible if you don't know what you are talking about.

Brown's Law: If the shoe fits, it's ugly.

Oliver's Law: A closed mouth gathers no feet.

Wilson's Law: As soon as you find a product that you really like, they will stop making it.

BCS Matters!

David Clarke

Next steps to professionalism

The future of IT is one in which the industry is populated by professionals, where the test of professionalism is related to business impact and outcomes, not just technical excellence.

The two key objectives of the BCS Professionalism programme are to increase professionalism by improving the ability of business and society to exploit the potential of information technology effectively and consistently; and to build an IT profession that is respected and valued for the contribution it makes to the exploitation and application of IT for the benefit of all - government, business leaders, IT employers, IT users and customers.

The ambition is to shape and create a mature IT profession with clearly defined professional standards that will bring with it recognition and respect for IT professionals and recognition for the importance of IT in business and the wider community.

After the successful launch of the programme in May of this year and the launch of the Prof IT alliance between BCS, e-skills UK, Intellect and NCC, the programme is moving forward to its second phase. This phase will be concerned with changing the practice and performance of individuals and organisations.

To do this key stakeholder groups are to be targeted and leaders identified to develop the vision and to ensure we work with organisations and individuals in all the areas we want to affect.

Five major campaigns are currently being proposed:

- Helping more businesses become IT capable in terms of exploiting and managing IT.
- Improving the professionalism of IT supplier organisations and thereby the performance of the IT supply chain as a whole.
- Growing the available pool of competent, professional IT practitioners both existing and future
- Making the IT profession itself more relevant, effective, i.e. achieving maturity
- Ensuring that the education and training sectors produce the knowledge and skills needed to support the above.

There is also a marketing job to be undertaken – we need to sustain interest in the importance of this work and make sure that the level of collaboration and cooperation across the IT sector that has generated the Professionalism in IT change programme will continue and, indeed, improve.

There are already many projects and activities taking place throughout the industry which will contribute to achieving the programme objectives but we want to directly encourage more organisations to start improving their IT exploitation capability thorugh collaborating with us.

The reality is that these changes won't happen overnight, nothing worthwhile does, but these objectives will be achieved by a very large number of individuals and organisations making a series of incremental changes.

In a recent article in ITNOW Peter Skyte of Amicus says that whilst we take it for granted that those in such occupations as teaching, medicine, nursing, architecture, law and accounting are regulated either by professional bodies or independent regulatory organisations it is easy to forget that this was not always the case. Such professionalism has in many cases had a long history of development, often arising from public scandal at the time and the resultant public outcry for 'something to be done'.

Our industry has had to endure being made a scapegoat for failed projects that are often not really attributable to the IT, but the principle of professionalism is supported by powerful arguments and BCS is pursuing this vigorously.

David Clarke is BCS CEO.

More information and comment on the BCS Professionalism Programme is at **www.bcs.org/professionalism**

To get involved in the programme please email Pam Latham, Professionalism Programme executive, via **profit@hq.bcs.org.uk**

Computer Forensics: A Valuable Audit Tool

Ryan Purita

Although computer forensics is a valuable tool for investigating cases involving fraud, many auditors are still unaware of the proper ways to conduct a forensic investigation and ways to ensure evidence is ready to be used in court.

Data breaches, hacking attacks, viruses, and insider threats are some of the security issues many companies face on a daily basis. Besides employing preventive measures, such as the use of firewalls and intrusion detection devices to prevent data breaches and thwart external attacks, many organizations around the world have been using computer forensics to identify instances of computer misuse and illegal intrusion. The use of computer forensic techniques also has flourished in the internal audit profession. However, many internal auditors are unaware of the advantages that computer forensics can bring to audit investigations. Learning how to acquire, analyze, and report data through the use of computer forensics can help auditors make the most of this investigative technique, as well as recover previously deleted documents that can provide the "smoking gun" needed to determine if a fraudulent activity took place.

THE FORENSIC INVESTIGATION

Computer forensics is the application of analytical techniques on digital media after a computer security incident has occurred. Its goal is to identify exactly what happened on a digital system and who was responsible through a structured, investigative approach. Forensic investigations cover all areas of computer misuse, including fraud, Internet and e-mail abuse, entry to pornographic Web sites, and hacking, as well as accidental deletions or alterations of data.

During the forensic investigation, evidence may be obtained in a variety of ways, including affidavits, search warrants, depositions, and expert testimony. Regardless of the means used to obtain data, examination of a computer or other device must be done thoroughly, carefully, and without changing anything. This ensures that the integrity of the original data and the evidence's validity are maintained.

If an internal auditor suspects fraud may have occurred, he or she should fill out an incident detection report form or similar document. The document needs to specify the date and time of the suspected fraud, who reported the incident, the nature of the incident, and the system(s) and application(s) involved. Once the incident is recorded, the auditor should inform the right company personnel, such as the chief information officer, chief security officer, chief information security officer, IT director, or human resources director. The person who needs to be contacted should be identified in the company's policies and procedures document. Note: It is important for companies to have an established, clear process for dealing with these kinds of incidents. This kind of pre-planning can help ensure that the proper channels are followed when an incident occurs.

Forensic investigations consist of three phases: acquiring the evidence, analyzing results, and reporting results. Below is a description of each.

Acquiring the Evidence

The process of securing or acquiring evidence starts with previewing the contents of a computer's hard drive or other media. To acquire the electronic data, including deleted information, the storage device must be mirrored or duplicated exactly bit by bit. The actual size or space of the storage device and transfer speed over a network cable will dictate the length of time needed to image the drive. Once the storage device is secured, a second device may be needed as a working copy if the original storage device was not seized or secured. This allows the examiner access to an unaltered copy of the electronic data.

The second step to collecting the evidence is the preview stage. Here, the auditor performs a simple check to determine the current status of data files. This can provide useful information about ownership of the data and its relevance to a particular investigation, as well as help to focus the subsequent investigation.

The third step when collecting evidence is to protect the data by capturing an exact copy of the original information. This is done through a process known as imaging. An image is an exact replica of the computer's hard drive or other media, and should include any slack space (for more information, refer to "What is Slack Space?" sidebar). The image is then investigated, rather than the original, to avoid altering the original data, which would make any evidence gathered inadmissible in court. Imaging is a vital step in a computer forensic investigation and is accepted as the best method for capturing computer evidence that may be presented in a court of law.

WHAT IS SLACK SPACE?

When an e-mail message is created, space is reserved in small sections. As the message grows, sections are added one at a time. These sections are of a specific size. When e-mail data is deleted, the space is available for use again, and new e-mails can use the sections as needed. If the new e-mail is shorter than the deleted e-mail, the storage device will contain sections with the previous data. This old written data is referred to as slack space. Here's a more general analogy: A person goes to the video store to buy a movie. The VHS tape allows for two hours of video to be recorded on it. The person decides that the movie is not worth keeping and uses the tape to record a 90-minute show. After taping over the original movie, the VHS tape still has 30 minutes of tape remaining, which contains the old movie.

Having captured an exact image of the data, the fourth step is to process it. All data must be processed, including deleted or partially overwritten files,

information hidden outside normal storage areas, and data in virtual memory and slack space. The most common method used by forensic examiners to capture this data is by using a write-blocking device. This device prevents the forensic examiner's machine from writing or altering the data on the suspect drive. Windows operating systems are notorious for this problem.

Typically, the suspect drive is removed from the machine if possible and plugged directly into the write-blocking device. Once this has occurred, an examiner can make what is called a "bit-stream" image of the drive. This is an exact bit-for-bit copy of the drive's contents, including deleted space, file slack, and logical files. Another method of capturing this data is using a Linux live CD or a boot disk, which allow the investigator to view the files on the drive, including deleted space and unallocated clusters, without altering the drive's contents. The examiner can then copy the files onto an external hard drive and view them. Hidden data often contains the most vital evidence to prove or disprove a case. In some cases, a file extraction may be appropriate. In other situations, a data index may be created to support powerful search tools.

After auditors have a complete image of the drive, they can start collecting the evidence. Most forensic software includes ready-made scripts for a variety of operating systems that automate certain functions such as encrypted registry parser, file finder, and file mounter. Because different programs may work better for different tasks, auditors should ensure organizations are using the right product based on their data analysis needs. For additional tips on how to gather evidence, refer to the "Additional Steps and Techniques" section below or "Steps to Handle Evidence During a Forensic Examination" sidebar.

STEPS TO HANDLE EVIDENCE DURING A FORENSIC EXAMINATION

1. Never work off the original image; create a backup for analysis.
2. Before working on a backup, hash it. Keep the original evidence in a safe.
3. Create a log of everyone who has access to the original evidence and copies.
4. Make notes of all findings, especially important ones.
5. Save often to prevent data losses in case of power outages.

Analyzing the Results

The second phase, analyzing the results, takes place after all the evidence is acquired and imaged properly. Because every case is different, auditors need to be fully trained when conducting a data analysis, or they should recommend a trained forensic examiner performs the evaluation if they lack the professional training to do so.

To analyze the evidence, auditors should use the working copy of retrieved, deleted, electronic data only, including files and folders. Auditors also need to maintain a chain of custody when handling the evidence. This enables them to ensure the legitimacy of the evidence presented in court is unquestionable and provides an audit trail of who accessed the data and when. To maintain a digital chain of custody, all images should be hashed — the process of creating a small digital fingerprint of the data.

During the data analysis stage, software also is used to inspect the raw data and organize it into an understandable report. As a result, the auditor must be able to tell the computer what to look for by using text-string search terms that will identify data pertaining to the specific incident under investigation. A search term should be created for each individual investigation and may be modified for each specific storage device within that investigation. Text strings could have as many as 500 words or phrases. The more text strings used, the better the results will be. Using more text strings, however, requires more work: As more text strings are used, results may contain a higher number of false positives or unrelated data that need to be examined. In addition, this process may take considerable time depending on the size of the storage device and the amount of data on that device.

Once the data is analyzed, auditors should review any information stored in special folders and files created by the operating system, in addition to folders and files created by the user. After this stage is completed, the evidence must be recorded, sorted into different classifications, and stored.

Reporting Results

The final phase of the forensic examination is creating the report and reporting the evidence. Final reports of the investigation should include a list of all the evidence gathered, a copy of printed documents listed as appendices, and an executive summary. In certain cases, (e.g., to obtain a search warrant or make a criminal charge), auditors may need to create interim reports. These reports are updated as new information is gathered and until the investigation is completed.

Report findings need to be ready to be used in a court of law. For instance, reports should clearly explain what made the company or auditor suspicious of the hard drive, how the hard drive was imaged, how the data was handled prior to the analysis, where within the hard drive the evidence was found, and what the evidence means. Internal

auditors who conduct the forensic examination should expect to be called to provide expert testimony during the court case and help the organization review the opposing counsel's evidence.

ADDITIONAL STEPS AND TECHNIQUES

Before and during the forensic investigation, internal auditors can take additional steps to ensure evidence is court-ready. Prior to the forensic examination, the auditor should physically secure the system in question and take pictures of the room, the area surrounding the system, and the system itself. In addition, the auditor needs to secure the evidence onsite or in a laboratory to ensure a proper chain of custody is followed and digital evidence is secured effectively. The auditor should also document all system details and any connections to the system, such as network cables and 802.11x connections.

The following actions should be avoided at all cost prior to collecting the evidence:

1. Modifying the time and date stamps of the system(s) containing the evidence before duplication takes place.
2. Executing non-trusted binaries by double-clicking or running any executable files that are on the computer (e.g., evidence.exe could be a wiping program that, when run, can destroy all the evidence on the drive).
3. Terminating the rogue process. This pertains to processes on the computer that are displayed when users press Ctrl+Alt+Delete. In hacking cases, it's common for people to press Ctrl+Alt+Delete and kill any processes they are unsure about. This may have adverse effects, such as wiping the drive or log files and notifying the attacker that the process has been discovered.
4. Updating the system before the forensic investigation takes place.
5. Not recording executed commands.
6. Installing software on the system.

Live Analysis

While collecting the evidence, a live or offline analysis can be performed as part of the gathering process. A live analysis takes place when the forensic investigation is conducted on the live system (i.e., the system is not powered down). Due to the volatile nature of digital media, auditors need to document all the steps taken while collecting the evidence during a live analysis. Besides refraining from installing software on the system, the auditor should not update the system with any security patches or hot fixes prior to imaging the drive. If the computer has any active windows open, pictures should be taken of the monitor as part of the examination's documentation, as well as the area by the system's clock to determine whether there are encrypted containers and, if so, whether they are open.

Internal auditors may encounter problems during any live analysis. Some of these problems include:

- Destruction or alteration of digital evidence by the auditor. Because computer files only get overwritten when data needs to take its place on the hard drive, clicking on files or folders on a computer will result in information being written to the drive, potentially overwriting valuable evidence. During a live analysis, this is unavoidable. To capture potentially overwritten data, the auditor should write every action performed on the system so that the forensic examiner can rule out that activity.
- Logic bombs and slag code. This refers to a piece of code or application that does something based on a condition. For example, wiping software commonly erases the drive on startup or shutdown. Therefore, the auditor can trigger a logic bomb or slag code simply by clicking on Start>Shutdown. The best way to avoid this situation is to unplug the machine from the wall. This will prevent software code from running, because the machine will have no electricity to run. If the investigation involves a laptop, after unplugging the machine, the investigator can shutdown the laptop by pressing the power button and holding it down for approximately five to 10 seconds. This will cut all power to the machine and force it to shutdown.
- Trojan binaries and root kits. Trojans and root kits are installed by the attacker. When operational, they send alerts to the hacker after a specific action takes place. Some Trojans even allow the attacker to view the computer screen in real time. Properly shutting down the machine, will prevent the hacker from seeing what the forensic investigator is doing. At a minimum, the computer's Internet connection must be disabled so that information is not sent to the attacker.
- No access to slack space, pagefile/hibernation files, Windows NT file system transaction logs, and print spoolers. Sometimes, these files may contain just the right evidence needed to prove a case. For instance, in cases involving the use of forged checks, printed files could have all the evidence needed. However, if the investigator is unable to access these files, the evidence could be lost as the investigation moves forward and files are imaged.

Once the data is gathered during the live analysis, the system must be imaged. Depending on the type of operating system, the auditor may need to shut down the system properly without damaging the evidence, while still allowing the system to boot up.

Offline Analysis

An offline analysis is when the investigation takes place on the imaged copy. When preparing the evidence, auditors need to know how to power down the system correctly. Some systems must be shut down properly, while others can be turned off by pulling the plug (refer to Table 1).

Pull the Plug	***Shut Down Properly***
Windows 95	Windows 2000 Server
Windows 98	UNIX- and Linux-based operating systems should be shut down properly to ensure that they boot up after imaging.
Windows Me	SCSI Raided Systems
Windows 2000	
Windows XP	
Windows 2003	

Table 1: Comparison of systems that can be turned off through the shut-down method or pull-the-plug method

When taking the system down, auditors need to make sure they remove the plug from the back of the computer and not the wall, because the computer may be plugged into an uninterruptible power supply. All cords attached to the computer, such as USB devices or network Ethernet cables, must be documented. Once the system is turned off and the information is recorded, the auditor might want to make an image of the system.

Auditors always should check to ensure duplication procedures and tools used meet the country's legal requirements. Otherwise, evidence may not be admissible in a court of law. For example, in the United States the National Institute of Standards and Technology requires that disk imaging tools used during the forensic examination meet certain standards, such as not altering the original disk in any way and logging all input and output errors.

WHAT'S NEXT?

A forensic investigation can be conducted on any device that stores electronic data, such as a computer hard drive, smart card, or palm pilot. Internal auditors can use computer evidence in a variety of crimes where incriminating documents can be found, including cases involving financial fraud, embezzlement, or data theft. A key point to remember during any forensic examination is that protection of the evidence is critical. Furthermore, the results of a forensic examination can be rewarding. Collecting evidence can allow organizations to respond to any problems immediately and authoritatively and to maintain the company's professional image.

Auditors who wish to learn more about computer forensics can visit the Computer Forensics, Cyber Crime, and Steganography Resources Web site, www.forensics.nl/. Besides finding information on computer forensics, auditors can search online for free forensic tools. A couple of good Web sites include:

- http://users.erols.com/gmgarner/forensics/: This Web site offers freeware forensic tools for Microsoft Windows platforms.
- http://ftimes.sourceforge.net/FTimes/index.shtml: The site takes visitors to the FTimes system base-lining and evidence collection tool.
- http://foundstone.com/resources/forensics.htm: This Web site provides links to different forensic tools, including Rifiuti, Vision, NTLast, and Forensic Toolkit.
- www.securityfocus.com/tools/525: The Security Focus Web page provides a link to AFind, a tool that lists a file's last access time without changing it.
- www.weirdkid.com/products/emailchemy/: This site provides a link to Emailchemy, a mail-format viewer program.
- http://ircr.tripod.com/: This site has a link to a Windows forensic tool that enables users to create an incident response collection report.

Ryan Purita, CISSP, ISSAP, ISSMP, EnCE works for Totally Connected Security Ltd. as the company's senior security specialist and forensic examiner. Purita has more than 10 years of experience working on strategies to counter external and internal information systems security threats. He has conducted forensic investigations, security audits, and risk assessments for clients in all industry sectors. Purita also has developed security products such as a surveillance system that connects wireless cameras via the Internet to a cell phone, laptop, or PC using 1344-bit military strength encryption.

Governing Data Governance

Lou Agosta

Data governance is the orchestration of a company's staff, technologies, and processes to transform data into an enterprise asset that yields business value for the organization. Data governance engages the policies and procedures specifying how decisions are made in handling data, how information resources are allocated and how accountability for results is tracked.

The analogy between governing the data in an enterprise and a system of checks and balances in a federal system of government is a useful one. Customers in market votes with their dollars and those managers and executives whose messages, products, and services win those dollars stay in office – keep their jobs. That is the ultimate check on the forward motion and balance of the enterprise. An executive function provides the leadership in setting priorities as to which projects, products, and data initiatives have the best chance of resonating with the market. A resource allocation function determines the hurdle – prospective return on investment – that must be surmounted by the executive initiative(s) to gain funding. At a high level, a compliance, monitoring, and auditing function – with a whole host of external regulatory agencies as well as Sarbanes Oxley, HIPAA, and Basel II — interpret the business practices as being consistent with the integrity and well being of the enterprise and customers alike. At an implementation level, project management keeps the initiative in line with the vision embodied in the governance model by surfacing issues and obstacles, working to resolve them, or escalating to request executive intervention to stop losses. All of this, of course, is easier said than done.

Since this is a short article, let's go straight to the heart of the matter. The weak link in data governance is between policy formulation and implementation. A data governance road map is the key to connecting the dots between the business and the technology in the IT department that is an essential part of implementing every business process. The road map winds it way through policies, standards, success criteria, key performance indicators, accountability and authority, and onto business results. The best data governance road maps trace a route that resembles a capability maturity model (CMM) – with a couple of differences.[1] The road map leads from the current state of enterprise data management capabilities in the direction of implementation. In contrast, a CMM leads from the heroics of the professional staff to the ideal state by means of a defined, repeatable, measurable, process of continuous improvement. Fewer heroics are good. Governance and CMM interact iteratively by means of incremental advances in capabilities enabling corresponding improvements in best practices in the implementation cycle. The road map moves from the cow path to the autobahn as implementation activities advance from readiness and engagement through integration to mastery. The goal is information availability – preferably with a low latency that maps to the requirements of the information demands of the business – thus, information on demand. Examples of policies that form the backbone for data governance look like this:

- Customers are our reason for existing as an enterprise. Customer data shall be managed as an enterprise resource independent of specific applications and as a source of value for the enterprise.
- Products (and services) are a key way the enterprise delivers value to our customers. Product data shall be managed as an enterprise resource independent of specific applications and as a source of value for customers.
- Data integrity is one of our most important products throughout the information supply chain. "Data integrity" means telling the truth about what is working and what isn't based on fact finding and defined processes. The quality of the data must be assessed periodically at the point of capture, transmission, summarization and aggregation, and decision making. Exceptions to quality must be documented as issues and worked through as a part of a process of continuous improvement.
- Professional staff shall focus on innovation and business value creation – and this regardless of whether the IT function is out sourced or managed in house. Management is responsible for assuring that defined processes and best practices, not heroics, are used in bring solutions based on data to business issues.
- Organizationally, an information management policy committee shall function as the equivalent of the legislative branch. It approves funding and procedural details. The information technology delivery organization shall function as the executive branch. It sees that policies and procedures are diligently designed and implemented. The auditing organization shall function as the judiciary branch of data governance. It makes the tough calls about compliance and what the policies really mean in specific real world contexts.

Obviously these examples are far from being a complete list.[2] In addition to a structure for governance, the policies must be operationalized. If not, policies will remain an idle wheel, not moving any other part of the enterprise, in a corporate ivory

[1] It is worth noting that the maturity framework out of which the CMM emerged was inspired by Philip Crosby's book *Quality is Free*. Crosby's quality management maturity frame describes five stages in adopting quality practices. This maturity framework was adapted to software by Ron Radice and Watts Humphrey at IBM, who subsequently brought it to the Software Engineering Institute

[2] For an example of what a more complete list might look like see *The Politics of Information Management: Policy Guidelines* by Paul A Strassmann, Information Economics Press, Connecticut: New Canaan, 1999. www.strassmann.com

tower along with the complete enterprise data model. That's why the road map was invented; and this article maintains such a road map is an essential part of any data governance initiative. For example, in the life of the database administration, data administration, or data management professional, heroics are common. The road map functions to get the professional staff off the tread mill of heroics and actually onto Figure 1. (Note that level zero, "heroics," is off the lower left end of the Figure). Initially, over-commitment is typical, and "tribal knowledge" and individual experience are the causes of success when success does occur (which is not often enough). The point of data governance is to move beyond heroics to a defined, repeatable, optimized process of managing the information supply chain. The staff are given permission and encouraged to tell the truth about data issues without risking dysfunctional organization behavior such as "shoot the messenger".

At stage one of data governance, data modeling, master data management, and reuse of data assets are incorporated into project discipline with sufficient rigor to repeat early successes with similar applications. But processes often differ between projects reducing opportunities for collaboration between teams and reuse of data models. Information is still occasionally subordinated and functionally dependent on applications, not treated as an enterprise asset. Internal clients (users) get visibility into the project at defined occasions such as data review and acceptance of major deliverables. This allows limited participation and control.

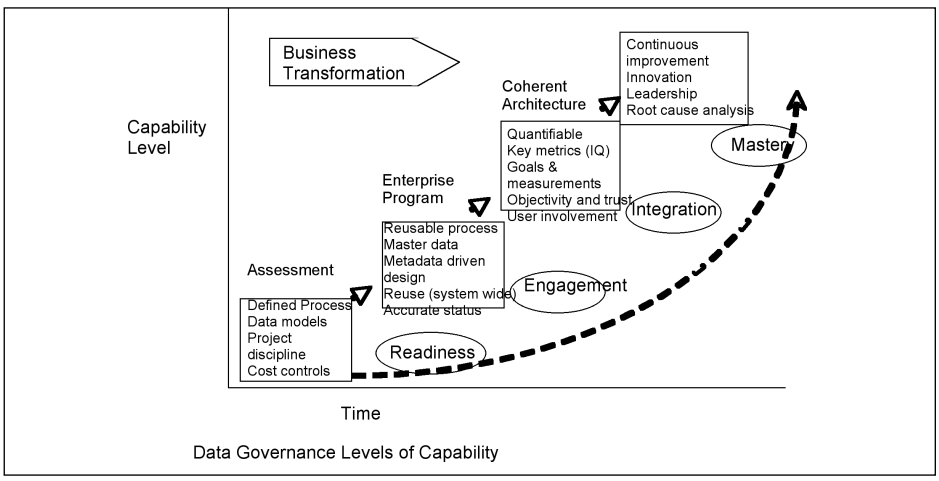
At stage two, a standard data management process is established, documented, integrated and adopted in operating the enterprise information supply chain. Data is managed as a corporate asset. This means customer, product, and other essential data dimensions are functionally decoupled from specific applications, which, in turn, can reuse these data assets. Leveraging a central repository or small set of federated repositories, metadata driven design is enabled. The data models and information represented by the metadata are able to be reused between systems, projects, and applications. Quality is a function of standards. The user is able to obtain accurate and quick status updates about data integrity and availability.

Level three of data governance establishes metrics on an enterprise-wide basis to the data governance process. This may have been done on a case-by-case basis previously. Now it is done systematically. Information quality is measured as a function of objectivity, usability, and the trustworthiness of data. Management establishes measurable goals and tracks progress toward them. Quality is a function of quantifiable standards. The user community is in a position to assess data management issues and risks prior to a project beginning or being implemented.

Finally, at level four, data governance enables continuous process improvement. Information quality metrics drive the design, piloting, and implementation of innovative ideas. Ways of packaging the data for revenue enhancement are discovered and rolled out. When data defects show up, root cause analysis rather than labor intensive inspect and remove is applied on a systematic basis. The commitment is to a data design for defect prevention. While the initial quality of some of the data captured is inevitably low, the result is "garbage in," "quality out." Collaboration between the data management professional and the user community occurs to establish a win-win relationship that looks beyond narrow departmental interests to benefit the whole enterprise and its customers. In the final analysis, "governance" turns out to be synonymous with "management" itself.

Lou Agosta, Ph.D., joined IBM WorldWide Business Intelligence Solutions in August 2005 as a BI strategist focusing on competitive dynamics. He is a former industry analyst with Giga Information Group, has served as an enterprise consultant with Greenbrier & Russel and has worked in the trenches as a database administrator in prior careers. His book The Essential Guide to Data Warehousing is published by Prentice Hall. Agosta may be reached at LoAgosta@us.ibm.com.

Reprinted with permission from DMReview.com Sept 14, 2006.



HUMOUR PAGE

George Costanza's 10 Commandments for 'Working Hard'

1 Never walk without a document in your hands. People with documents in their hands look like hardworking employees heading for important meetings. People with nothing in their hands look like they're heading for the cafeteria. People with a newspaper in their hand look like they're heading for the toilet. Above all, make sure you carry loads of stuff home with you at night, thus generating the false impression that you work longer hours than you do.

2 Use computers to look busy. Any time you use a computer, it looks like "work" to the casual observer. You can send and receive personal e-mail, chat, and generally have a blast without doing anything remotely related to work. These aren't exactly the societal benefits that the proponents of the computer revolution would like to talk about but they're not bad either. When you get caught by your boss — and you will get caught — your best defence is to claim you're teaching yourself to use new software, thus saving valuable training dollars.

3 Keep a messy desk. Top management can get away with a clean desk. For the rest of us, it looks like we're not working hard enough. Build huge piles of documents around your workspace. To the observer, last year's work looks the same as today's work; it's volume that counts. Pile them high and wide. If you know somebody is coming to your cubicle, bury the document you'll need halfway down in an existing stack and rummage for it when he/she arrives.

4 Use voice mail. Never answer your phone if you have voice mail. People don't call you just because they want to give you something for nothing — they call because they want you to do work for them. That's no way to live. Screen all your calls through voice mail. If somebody leaves a voice-mail message for you and it sounds like impending work, respond during lunch hour when you know they're not there — it looks like you're hardworking and conscientious even though you're being a devious weasel.

5 Look impatient & annoyed. One should also always try to look impatient and annoyed to give your bosses the impression that you are always busy.

6 Leave the office late. Always leave the office late, especially when the boss is still around. You could read magazines and storybooks that you always wanted to read but have no time until late before leaving. Make sure you walk past the boss' room on your way out. Send important e-mail at unearthly hours (e.g. 9:35 p.m., 7:05 a.m., etc.) and during public holidays.

7 Use sighing for effect. Sigh loudly when there are many people around, giving the impression that you are under extreme pressure.

8 Opt for the stacking strategy. It is not enough to pile lots of documents on the table. Put lots of books on the floor etc. (thick computer manuals are the best).

9 Build your vocabulary. Read up on some computer magazines and pick out all the jargon and new products. Use the phrases freely when in conversation with bosses. Remember; they don't have to understand what you say, but you sure sound impressive.

10 Don't get caught. MOST IMPORTANT: Don't forward this to your boss by mistake!

The top eight unintentionally worst company URLs

Everyone knows that if you are going to operate a business in today's world you need a domain name. It is advisable to look at the domain name selected as other see it and not just as you think it looks. Failure to do this may result in situations such as the following (legitimate) companies who deal in everyday humdrum products and services but clearly didn't give their domain names enough consideration:

1. A site called 'Who Represents' where you can find the name of the agent that represents a celebrity. Their domain name. wait for it. Is **www.whorepresents.com**

2. Experts Exchange, a knowledge base where programmers can exchange advice and views at **www.expertsexchange.com**

3. Looking for a pen? Look no further than Pen Island at **www.penisland.net**

4. Need a therapist? Try Therapist Finder at **www.therapistfinder.com**

5. Then of course, there's the Italian Power Generator company – **www.powergenitalia.com**

6. And now, we have the Mole Station Native Nursery, based in New South Wales : **www.molestationnursery.com**

7. Welcome to the First Cumming Methodist Church. Their web site is – **www.cummingfirst.com**

8. Then, of course, there's these brainless art designers, and their whacky web site: **www.speedofart.com**

The most important IT controls for a small business
(an empirical study)

Bruce (Harv) Busta, Kris Portz, Joel Strong, Roger Lewis

For small businesses, controlling Information Technology (IT) risks is a great challenge. Often resources are limited for IT controls; however, a compromised IT control can have a devastating impact. In such a situation merely a financial loss is the best-case scenario. Worse-case scenario can include the loss of customers or possibly the shut down of operations.

Every company has a large number of IT risks for which to control, but prioritizing which risks to control for is probably more acute for small business because of their limited resources and IT staff. This paper presents a research study which has tried to identify the most important IT controls for small businesses.

Defining a Small Business

We used IT experts to determine the top IT controls. To ensure that all participants in our study had a similar definition of a "small business" and a common understanding of both the technology and IT skills available to a small business, we asked participants to visualize a small construction company with 25 employees.

Specifically, they were asked to imagine a company that had the following personnel structure:

- The owner – who oversees all aspects of the business.
- Two sales/customer service personnel.
- One bookkeeper
- One secretary/receptionist
- One warehouse/materials manager
- Three construction supervisors
- Fifteen construction workers

The participants were asked to assume that this illustrative small business had the following scenarios related to technology:

- Twelve computers which are connected to the Internet, some with a wireless connection.
- E-mail is an essential form of communication with vendors and customers.
- A self-employed computer consultant is hired for technical IT tasks. Periodically, this individual is used to install new computers/software, manage the network and provide training.
- Off-the-shelf software is used.
- Backup of data is done periodically by the bookkeeper.

The purpose of this description was to make sure that the participants had a similar size, technology sophistication, and IT risk level in mind when they evaluated the controls which were most important to a small business. The participants were told to use this description as an example; that is, they were not to determine the IT controls for this specific small business, but rather small businesses in general.[1]

The Data Collection Method

To identify the top IT controls for small businesses, we used a Delphi survey.[2] A Delphi survey uses a panel of 10-12 experts, multiple surveys and an anonymous feedback process to find its results. The strength of the Delphi method is that it produces a well-considered consensus on subjective and complicated issues.[3]

In round one of our study, experts were asked to rank the top 10 IT controls from a list of 30 possible controls[4] (See Figure 1). Our list of controls was created from the control objectives of the 3rd edition of COBIT. We slightly modified the control objectives so that they were well adapted for a small business.

In addition to selecting what they thought were the 10 most important controls, the experts could provide comments on the various controls, seek more information, or suggest additional controls through a discussion board.

After providing their first round responses, the experts received the top 10 rankings for the group compared to their individual responses. They were then instructed to reevaluate their rankings given this new information. The experts were encouraged to share their insights on the overall rankings and/or a specific control. They could anonymously "lobby" the group for a control that they thought was important. This is an important feature of the Delphi survey, in that it allows the experts to share their insights so the group can benefit from their collective knowledge. The anonymous format overcomes the problems of leadership bias, face-to-face confrontation and group dynamics.

Additional rounds are completed until a stable consensus is achieved. During all rounds the experts can provide comments and share insights in

The Experts

Our global panel of experts was very experienced with IT controls. Additionally, some had considerable experience in the construction industry and/or with small businesses.

Anonymous, East Coast, USA

Melissa Brown
Solutions Consultant,
Microsoft Business Solutions Certified Master
Inetium -- Business Intimate Technology Solutions
St. Cloud, Minnesota

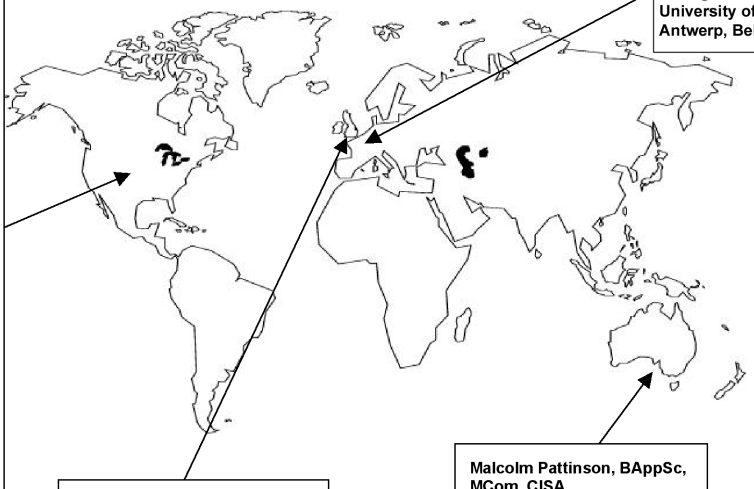
Christopher P. Buse, CPA, CIA, CISA, CISSP
Information Technology Audit Manager
Minnesota Office of the Legislative Auditor
St. Paul, Minnesota

Jim Freeland, CISA, CISSP
Information Security Risk Management
UnitedHealth Technologies
Minneapolis, Minnesota

Diane Kuechle
Computer Resources Unlimited, Inc
St. Cloud, Minnesota

Craig Olsen, CPA, Principal
LarsonAllen Construction Group
LarsonAllen CPAs, Consultants and Advisors
Minneapolis, Minnesota

Neil Thomas, CISSP, CISM, IAM/IEM
Senior Security Consultant
Eide Bailly Technology Consulting
Bloomington, Minnesota



Prof. Dr. Wim Van Grembergen
Information Systems Management
University of Antwerp
Antwerp, Belgium

John A Mitchell, PhD, MBA, CEng, CITP, FBCS, MBCS, FIIA, MIIA, CISA, QiCA, CFE

Managing Director
LHS Business Control - Corporate Governance Specialists
Hertfordshire, England

Malcolm Pattinson, BAppSc, MCom, CISA.
School of Computer and Information Sciences
University of South Australia
Adelaide, South Australia

Figure 1 – 30 IT Control Objectives originally presented to the Delphi experts[5]

IT Controls

PLANNING & ORGANIZATION

1. IT as Part of the Organization's Long – and Short-Range Plan
2. Adequate IT Staffing Levels
3. Well Trained and Cross-Trained IT Personnel
4. General Employee IT Security Training Program
5. General Employee IT Data Integrity Training Program
6. Job Change and Termination Procedures
7. Risk Evaluation Program

ACQUISITION & IMPLEMENTATION

8. Software Acquisition Procedures
9. Software Scalability Reviews
10. Software Installation Procedures
11. Software Change Procedures
12. Software Documentation Policy
13. Software Update Procedures

DELIVERY & SUPPORT

14. Out-Sourced IT Support – Clearly Defined Contracts
15. IT Continuity and Recovery Plan
16. Back-up Procedures
17. Identification and Authentication Procedures
18. File Access Privilege Controls
19. Network Security
20. Viruses Protection
21. Prohibition of Unauthorized Software
22. Software Accountability Procedures
23. Problem Reporting and Resolution Procedures
24. Data Input Controls
25. Data Output Controls
26. Protection of Disposed Sensitive Information
27. Physical Security of Hardware
28. Uninterruptible Power Supply
29. Robust Remote Operation Controls

MONITORING

30. Monitor the Process

an anonymous format. In our study, the Delphi survey was conducted using the Internet and a web-based educational tool.

The Most Important IT Controls

After three Delphi rounds it was revealed that there are 11 key controls for small businesses. In terms of importance, these key controls fall into three distinct groups, which we have labeled "Gold," "Silver" and "Bronze." See Figure 2.

The three most important IT controls for a small business are:

- ✔ Updated firewalls and secure wireless connections.
- ✔ Up-to-date Virus and Spyware protection.
- ✔ Regular and TESTED Back-up Procedures.

The authors found it interesting that during the Delphi rounds none of the experts discussed the importance or asked clarifying questions about these top three controls. It appeared that the importance of these topics was unanimous and well understood.

The silver group contains five controls of similar importance.

- ✔ File Access Privilege Controls - Prohibiting individuals from accessing specific files which they do not need to use. For example, sales people would be prohibited from entering the payroll module.
- ✔ IT as Part of the Organization's Long- and Short-Range Plan - This control ensures that technology enhances and supports the businesses' strategy. If quality is a central strategy, the computer system should be configured to support this goal (i.e., data accuracy will be verified by several methods). Rather, if price or quickness are central strategies, different technologies and controls will be used than if quality is the primary goal.
- ✔ IT Continuity and Recovery Plan - A disaster recovery plan is important for small businesses, even if it is very basic.
- ✔ Identification and Authentication Procedures - Complex passwords, confidential passwords and regularly changed passwords are important.
- ✔ Management Support/Buy-In - The owner of the organization must provide leadership and financial support for IT controls.

The bronze group contains the following three controls:

- ✔ Risk Evaluation Program - Small business should periodically evaluate the wide range of IT risks they face (i.e., a software "bug" which could result in an error in a bid or contract or a spreadsheet error which results in an incorrect decision) and rank them in terms of magnitude. This can simply be a brainstorming session, but when done periodically it can be powerful.
- ✔ General Employee IT Security Training Program - All employees should be trained on the importance of IT security and how to implement strong confidential passwords. They should also practice good security with e-mail attachments and when downloading files.
- ✔ Data Input Controls - Controls that verify that inputted data is correct are critical. For example, field formats (xxx-xxx-xxxx) for phone numbers and zip codes increase data accuracy. This is especially important for part numbers. Additionally, a reasonable range test for sales price or quantity assists in accurate data input.

Figure 2

The 11 Most Important IT Controls as Determined by the IT Experts	Round 3 Group Ranking
19. Network Security	1
20. Viruses Protection	2
16. Back-up Procedures	3
18. File Access Privilege Controls	4
1. IT as Part of the Organization's Long- and Short-Range Plan	5
15. IT Continuity and Recovery Plan	6
17. Identification and Authentication Procedures	7
A. Management Support/Buy-In	8
7. Risk Evaluation Program	9
4. General Employee IT Security Training Program	10
24. Data Input Controls	11

The Contentious IT Control

- ✔ Software Scalability Reviews - One IT control that did not make it into the top 11 was Software Scaling (ensuring that software is capable of meeting future needs for increased data processing, networking, etc.). The panelists were highly divided on this control. Three panelists ranked this control very high, while two ranked it very low. The other panelists were neutral. Despite "lobbying" by two of the panelists this control did not rank highly. Interestingly, the three panelists who ranked it highly all have extensive experience with small businesses; conversely, those who ranked it low, were from medium to larger enterprises. Because of this strong difference of opinion this control is not ranked in the top 11; however, it is the authors' opinion that this is a control that is often overlooked for rapidly growing small businesses.

Conclusion

For small businesses, maintaining an effective IT control system can be a significant and costly challenge. Yet, this is a vital task for small businesses. Using a group of IT experts and an established research method we have identified the top 11 IT controls for small businesses. This list can be used to guide IT control expenditures.

First and foremost, network security (updated firewalls and secure wireless connections), virus and spyware protection and back-up procedures should be in place. These were the undisputed "Big Three" and should be in operational in every small business.

After the above three controls are established small businesses should evaluate the following IT controls:

- ✔ File Access Privilege Controls
- ✔ IT as Part of the Organization's Long- and Short-Range Plan
- ✔ IT Continuity and Recovery Plan
- ✔ Identification and Authentication Procedures
- ✔ Management Support/Buy-In

A small business owner is not likely to be familiar with File Access Privilege Controls, IT as Part of the Organization's Long- and Short-Range Plan and IT Continuity and Recovery Plans. It will be incumbent for the IT consultant to help the small business owner recognize the importance of these controls, understand them and work closely with the business owner to put these controls in place.

Once the above five controls are in functioning within the small business, management should work to implement a Risk Evaluation Program, General IT Security Training Program and effective Data Input controls. Also, if the company is experiencing rapid growth the Scalability of Software should be evaluated.

Interestingly, several of these key controls are not straightforward technological solutions. Determining the organization's short-term/long-term IT plan, developing a continuity plan, management's support of IT controls and a risk evaluation program are controls that require considerable cooperation, business knowledge and interpersonal skills by management and the IT consultant.

Although the implementation of these 11 controls will be a significant undertaking for some small businesses, our research indicates that these are the most critical controls for a small business. By executing these 11 controls a small business can greatly improve the security, reliability, strategic usage and accuracy of its IT resources.

Endnotes

[1] During the Pre-Test of the Delphi instrument, IT Experts validated that the description of the small business IT environment was realistic and typical.

[2] The Delphi method was developed in the 1950's at the Rand Corporation to help forecast the impact of technology during the cold war. (See Wikipedia - "Delphi Method")

[3] Helmer-Hirschberg, Olaf; *Analysis of the Future : The Delphi Method*, RAND Paper Document Number: P-3558, 1967.

[4] In essence, the experts were asked to trade off the importance of various IT controls. Fletcher and Verschoor (1984) and Horton and Pruden (1988) have successfully used the Delphi method to determine similar tradeoffs.

Fletcher, J. C., and C. C. Verschoor. 1984. "How to determine the social costs and benefits of business decisions: a railroad industry study." Managerial Planning 33 (September/October): 10-13, 21.

Horton Jr., F. W., and Pruden, J. S. 1988. "Benefit: cost analysis — a delphi approach." Information Management Review 3 (Spring): 47-54.

[5] For a detailed description of these 30 control objectives, see: http://web.stcloudstate.edu/babusta/Detailed_description_of_the_30_controls_originally_presented_to_the_Delphi_experts.htm

Bruce (Harv) Busta, Ph.D., CPA (inactive), CISA
Chairperson and Professor of Accounting
Department of Accounting
G. R. Herberger College of Business
St. Cloud State University
St. Cloud, Minnesota 56301 USA
Harv@stcloudstate.edu

Kris Portz, Ph.D., CPA
Associate Professor of Accounting
Department of Accounting
G. R. Herberger College of Business
St. Cloud State University
St. Cloud, Minnesota 56301 USA

Joel Strong, Ph.D., CPA
Associate Professor of Accounting
Department of Accounting
G. R. Herberger College of Business
St. Cloud State University
St. Cloud, Minnesota 56301 USA

Roger Lewis, MS, CPA
Instructor of Accounting
Department of Accounting
G. R. Herberger College of Business
St. Cloud State University
St. Cloud, Minnesota 56301 USA

Bruce Busta, PhD, CPA, CISA
teaches IT auditing and accounting information systems. He is a professor of accounting and the chairperson of the department of accounting at St. Cloud State University. He is the ISACA Academic Advocate on the St. Cloud State University campus and a member of Information Systems Audit and Control Association (ISACA), Minnesota Society of CPAs, and the American Accounting Association.

Kris Portz, PhD, CPA
is an associate professor of accounting at St. Cloud State University where she teaches accounting information systems. Her research interests include assurance services, auditing, system security and accounting education. Her research has been accepted for publication in the Review for Accounting Information Systems and The CPA Journal.

Joel Strong, PhD, CPA
teaches IT auditing, accounting information systems and managerial accounting at St. Cloud State University. He is an associate professor of accounting. His research interests include assurance services, auditing, managerial accounting and accounting education. He has recently published articles in Advances in Accounting, The Review of Business Information Systems, The CPA Journal, and Research in Governmental and Nonprofit Accounting.

Roger Lewis, MS, CPA
has over ten years of experience as a certified public accountant, along with industry experience in the manufacturing, real estate, construction, and automotive settings. He is a member of the American Institute of Certified Public Accountants and Arizona Society of Certified Public Accountants.

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	Vacant	
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Vacant	
JOURNAL EDITOR	John Mitchell	john@lhscontrol.com
WEBMASTER	Allan Boardman	allan@internetworking4u.co.uk
EVENTS PROGRAMME CONSULTANT	Vacant	
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**	Members' area Userid = irmalondon Password = 4members06

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)*	£25
INDIVIDUAL MEMBERSHIP *(A members of the BCS)* BCS membership number: _____	£15
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 2 = External Audit 3 = Data Processor 4 = Academic 5 = Full-Time Student 6 = Other (please specify)
SIGNATURE: DATE:

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

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

BCS IRMA SPECIALIST GROUP ADVERTISING RATES

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

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

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

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

Display Advertisements Rates:

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

Direct e-mailing

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

Contact

Administration

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

Meeting Venue unless otherwise stated

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