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

JOURNAL
volume 14 number 2 spring 2004 ISSN 1741-4229

Programme for members' meetings 2004

Wednesday 28th January

COMPUTER AUDIT BASICS, PART I

Before deciding how and when to audit a system or process, you need first to know what you are auditing and why. This meeting provides answers to the strategic questions: "what" and "why". This meeting is addressed by a person with many years experience in computer audit management.

Late Afternoon
16.00 for 16.30
to 18.00
KPMG

Tuesday 17th February

NETWORK MANAGEMENT and SECURITY

A typical organisation's network links customers, office staff, home workers, suppliers and the public to vital information ystems and internal websites, as well as providing the basic infrastructure for essential services like email. Any failure of the network is both very visible and extremely disruptive. This seminar provides some answers to the question of how to approach an audit of the network.

Full Day
10.00 to 16.00
Old Sessions
House

Tuesday 16th March

OUTSOURCING

This seminar introduces you to outsourcing. It shows how to maximise benefits from outsourcing whilst taking care of the security and risk/audit issues. You will proceed through the outsourcing life cycle from the intitial management decision to outsource through the negotiation stage to the implementation and management stage. A range of management solutions and checklists are introduced and cases taken from real-life outsourcing contracts will illustrate the seminar.

Full Day
10.00 to 16.00
Old Sessions
House

Tuesday 11th May

SERVER FARMS

IRMA AGM precedes the meeting

Today many companies have installed Server Farms as a solution to their server requirements. The meeting will outline what a Server Farm consists of and why it is seen as a solution to a company's processing needs plus: the benefits and drawbacks; the most common problems arising during implementation; the controls appropriate to maintenance; issues surrounding support.

Late Afternoon
16.00 for 16.30
to 18.00
KPMG

Please note that these are provisional details and are subject to change.

The late afternoon meetings are free of charge to members.

For full day briefings a modest, very competitive charge is made to cover both lunch and a full printed delegate's pack.

For venue maps see back cover.

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 June	Winter Edition	7th November

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

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

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

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

Editorial

The world of regulation is getting tougher. Each year the Government attempts to enact between twenty and thirty new statutes that effectively make you or your company a criminal in areas where you weren't so last year. On top of that the EU issues around twelve hundred new directives which, when subsumed into UK law, have a similar effect. Then we have all the new regulatory requirements from such organisations as the Financial Services Authority. Not to forget the voluntary stuff that we sign up to in the guise of ISO9000 and ISO17799. All in all there is a mountain of compliance to adhere to and the mountain is getting bigger each year. Turnbull got it right when he wrote that compliance was a key internal control requirement for organisations. Indeed, so great is the problem for those involved in information security that I have added compliance to the Confidentiality, Integrity and Availability triad. At least the acronym CIAC moves us away from apparently being an arm of a sinister secret service type of organisation, but more importantly it raises the profile of information security from being something that is 'nice to have' to being something that is essential to doing business. It's not uncommon these days to see IS auditor jobs being advertised with 'CISA or QiCA preferred' prominently displayed and soon IS security managers will be faced with 'CISM or CISSP required'. Likewise, contracts for supplying IS services will require 'ISO17799 accredited'. In the world of regulation, having the appropriate qualification or accreditation will become an essential requirement for doing the work. This is because organisations, in order to show that they operate to best practice, will want themselves, or their staff, to be able to prove that they meet the appropriate regulatory requirement. So, if you expect to progress in the IS audit or security fields you will have to seriously consider obtaining a professional qualification. Even if you have an MSc in IS auditing, you will be forced to obtain yet another piece of paper to add to that already impressive list on your CV. So why is he banging on about qualifications I hear you ask?

The answer lies in the 'BCS Matters!' column of this Journal. Colin Thompson explains the new BCS membership structure, which has been partly designed with the members of its specialist Groups in mind. Many of you may think that you do not have the qualifications or experience to become a chartered MBCS member of the Society and until now you may have been right. But the world is changing and as Colin explains, applicants for MBCS will now only need a maximum of 5 years ICT experience even if you hold no recognised academic qualification. The speed of processing has also been enhanced so you will not have to wait for ages after making your application. The fact that you are member of this group indicates that you probably work in the IS auditing or security field and as every letter after your name gives you an edge in the job progression game, I urge you to examine the new membership structure to see whether you are now eligible to become an MBCS.

Coincidentally, Bob Ashton in his 'Down Under' column reports on a situation where someone using the CISA designation had failed to do the mandatory CPE requirement and the designation had lapsed as a result. The need for qualifications to be checked at employment commencement is recommended in ISO17799, but as Bob points out there is no requirement to check that the qualification remain valid. Something to think about the next time you place an advertisement with a 'CISA preferred' sticker on it.

Our own Deputy Chairman, Alex Brewer, has crafted an article on programming using PERL, which as an old COBOL code writer I found particularly interesting. Open source is becoming a real competitor to the domination of Microsoft, so anything that raises its profile is to be welcomed.

The problems associated with the control of office applications, especially spreadsheets, is dealt with by Steve Semenzato. This is a timely reminder that no matter how well the main application is controlled, the real risks lie with the use made of the data by the end user with the (usually) poorly controlled spreadsheet. Many of you will remember a survey by one of the big four that a third of the spreadsheets that they examined contained a material error, so anything that can help in this area is to be welcomed.

How many times have you been told that your finding regarding a violation of your company's security policy is correct, but compliance is not immediately possible and therefore a waiver will be made? More times than you are comfortable with I expect.

Gordon Smith tackles this subject with his usual verve and shows that ultimately the cumulative effect may expose the company to breaches of compliance legislation.

Many auditors now get involved in special investigations where the evidential requirement is often higher than for normal audit work. Also, the investigation may require the evaluation of many different aspects of a situation which at first sight bear no relation to each other. In order to help you in these situations I have arranged for a number of articles to be published in this and the next few editions that cover the various aspects of these investigations. In this edition we start the process with an article by Greg Krehel on the need to get your case into chronological sequence and another by Priscilla Emery dealing with the email archiving nightmare. These are complemented by Clive Carmichael-Jones' article on email forensics.

Jean Morgan, our Treasurer, gives an update on our finances and also asks whether anyone is interested in tutoring a new MSc in Information Security that is being developed by the Open University. Now that would look good on your CV.

Mark Smith has negotiated some substantial discounts on useful audit software packages. You will find details later in this edition, but the savings more than make up for your modest membership subscription.

I am off to Zurich for a week of conferencing. Well, someone has to do it!

John Mitchell

Pearls of Wisdom
The PERL Programming Language

Alex Brewer

Do you want to learn a powerful programming language? Would you like the work you develop to be taken with you and run in almost any environment (except Palm Pilot and one or two others)? Do you want to take other people's work and plug it into your work rather than write all of your requirements from scratch? Is your data resident on SQL databases, or mainframe or PC text files? Do you need to churn through large files to extract or summarise something of interest? Do you want to be really mean and not spend any money on the software to boot?

Then Perl is for you!

In addition there are graphical add-ons for Windows and Linux, so your Perl script can be used to realise rapid developments in these environments.

If your company uses an IBM mainframe or AS/400, or if your organisation uses Tandem Guardian or Sun kit, or if you have a Compaq palmtop or a Psion organiser, you will find a version of Perl to run on them all.

There is what may be an urban myth about about an UCLA programming contest where the winner decidedly trounced all others by using Perl. It is said that the organizers of the contest banned Perl from subsequent contests, and that the winner didn't know what to do with his prize – a copy of Microsoft Visual C++!

Whether or not this myth is true, it illustrates that the language is effective, and because of that is widely used both in business and public service. Perl programmers are proud of describing their chosen language as the programming equivalent of a Swiss army knife – indeed one writer overdoes it and refers to a Swiss army chainsaw!

What does the name mean?

The acronym PERL is officially based on "Practical Extraction and Report Language", however other names exist, including "Pathologically Eclectic Rubbish Lister".

History

Larry Wall designed Perl as part of a long defunct NSA project (Blacker) whose requirements came out of the disciplines of linguistics, art, common sense, computer science and probably spying! Drawing on the best features of the computer languages available at the time, he created the first version of what became Perl.

He pulled in features from c, sed, awk and shell, as well as more minor contributions from ada, lisp and Basic.

As writer of the open source unix newreader program (rn) Larry realised that Perl was the ideal candidate for an open source project, putting it out to the comp.sources.misc newsgroup in 1987. This was done on the basis that 'it is much easier to ask forgiveness than to seek permission'! With companies more concerned to enforce intellectual property rights one wonders if he would have got away with this today.

The language has since been updated to include many more functions and has been ported to many environments.

Usage

CGI (Common Gateway Interface) scripting generally uses Perl to extend the capability of web server and browser interaction by inserting programs between the browser and server to make the contents interactive. This includes such items as hit counters, drawing in data from legacy systems and writing to and from bulletin boards.

One area that Perl excels at but which receives little attention is that of data handling and formatting. Perl is adept at retrieving data from a wide variety of forms and then transforming it into something acceptable to a downstream system. It is particularly adept at this in the unix environment, where perl scripts can be called from the command line like any other unix function.

To see Perl at work, go to any page on the BBC website and look for the Text-Only link. When you click on this link, the page converts to a basic format with text and links, gone are all of

the frames and pictures. The program that drives this is a Perl script called Betsie. The BBC has a huge website, and faced with the mammoth task of converting all of their pages to text format (required for public broadcaster accessibility and also to comply with the disability discrimination act), they chose instead to develop a Perl script to convert the pages on the fly. The BBC use Perl in this way on one of the busiest sites in the world. They surely use it in other ways, but this is the easiest to find.

Finding data (Regular Expressions)

Perl uses a concept called a 'regular expression' to define how data are identified within any type of file. These expressions are similar in concept to Left, Mid and Right in Excel but are far and away more flexible. You can search for a match (or non-match) with a group of characters (or characters not in the group) which may appear at the beginning/end of a word/line/block of data, and additionally, the characters/phrase can repeat.

These objectives are achievable with enough conditions and filters in many languages, however in Perl, it is often possible to perform many such operations in a single line of code.

Speed

Perl is an interpreted language and is not compiled before run time. The core modules of the Perl interpreter are written (and compiled) in C. This then runs Perl scripts written by users, which are simply text files.

The compiled parts of Perl have been configured to optimise the way in which the operations are performed, so that a badly written script is implemented in a 'this works exactly the same way but faster' manner.

The result of being based on C executables and optimising the execution of scripts is that Perl is very quick. A number of mission critical applications I have seen in my time as a system auditor use Perl as the means of passing data between users and servers, as well as data between applications. The manager of an ISP told me that when he upgraded his server's log monitoring software to a Perl based tool, the first time he ran it he thought it had failed because it happened so fast, but it had in fact finished!

Plug ins

The heart of the Perl licence is open source, and responding to that many users have chosen to release their scripts under open source licences. Many of these have been packed into perl modules (a module is simply a text based script given a name which ends in ".pm" and passes data back and forth in a standard manner).

Many of these modules are available online in the CPAN archive, a repository for Perl knowledge sharing. After inserting a line like 'use TheModuleOfYourChoice.pm' you can draw that person's work into your scripts. There are hundreds, or more likely thousands, of such modules on the CPAN site offering functions from the sublime to the ridiculous which are updated daily.

Picking some items at random from the daily list at the time of writing found some tools for configuring Cisco routers, a software version control system and routines for writing to a Btrieve database.

Other examples of perhaps more useful modules are routines dealing with retrieving data from SQL databases (Oracle, MySQL, SQL server etc.), passing data to and from the internet, and time handling routines.

What will it run on?

Perl runs on a huge number of platforms which means that skills as well as programs developed on one platform can be transferred to another one.

There are a number of builds of Perl for the Windows/DOS environment, however one of the most popular is ActiveState. Unix and Mac OSX users (and many other environments) will find Perl already installed with the operating system.

It's probably quicker to define what it does not run on. Perl does not run (yet) on Inferno, OS1100, PalmOS, PRIMOS or VxWorks. Bad news for public sector mainframers: although it is omitted on the CPAN site, I don't think there is a VME version (if there is, please let me know).

Security considerations

Being an interpreted language rather than a compiled one, the security considerations are different from a compiled language. One common control is for only compiled source code and no compilers to be available in the production environment. This prevents users developing and running their own code in production.

However Perl side steps this control as the interpreter runs scripts (text files) which can generally be found in the production environment.

Providing access to servers with Perl installed and having vulnerable data available is a recipe which allows Perl scripts to be developed in production to help compromise a business's infrastructure.

It follows that the Perl interpreter needs to be secured in whichever environment it is installed so that access to it is appropriately restricted. It is also necessary to secure the data as well as Perl, or it will be vulnerable to being programmatically corrupted/altered by a Perl script.

Obviously the scripts themselves used for production processing need to be secured so that they cannot be modified to perform unauthorised functions.

Badly written Perl CGI scripts can be used to compromise the web server that they are installed on, however the remedy for this is available on the internet. Ask a newsgroup for details. The default CGI scripts installed with an operating system should be removed from a live web server, and only the minimum scripts required actually installed.

There are also Perl scripts written by hackers to compromise security, so even the black hats use Perl!

Cost

As discussed above, the project is open source, so the cost of the software itself is time, training, some good books, and a donation to the project, if you wish!

Support

There are a number of excellent books about Perl. The most famous one is known as 'the camel', after the animal that was chosen for the cover of the first edition of 'Programming Perl'. The current edition remains the standard reference book for Perl programmers, and the camel remains the logo for Perl.

You will need access to the internet to get support for a particular problem. This is because the best forms of support are via mailing lists or internet newsgroups. The groups are knowledgeable, enthusiastic and responsive.

There are Perl Monger mailing list groups all round the world. Obviously it pays dividends to follow newsgroup etiquette to get the best response. This would include researching the Frequently Asked Question lists and other reference material before asking your question.

Weird stuff

Because of its flexibility, Perl can be adapted to many styles of programming. Novices (like me) can write many comments and use too many variables to keep the processing clear to other novices (especially auditors).

Perl professionals can write complex programs in a matter of five lines, where the function is not clear to an outsider, or indeed another Perl programmer.

Reflecting this idiom there are regular contests in the Perl community to write code which nobody else can understand (the Perl Obfuscation contest) and even Perl poetry contests – at the time of writing there is a Perl haiku contest, one part of which includes a condition that the haiku must run as a valid program.

Conclusion

If you are one of those people who would like to learn a programming language, but can't decide which one, I would suggest Perl. Fast, freely available, and genuinely powerful, it is unlikely to go out of fashion, being part of the open source community's LAMP (Linux, Apache, MySql and Perl) environment. Proven in battle and widely used, Perl has much to recommend it.

Sources

Data Munging with Perl (Cross)
Perl in a Nutshell (Siever, Spainhour & Patwardhan)
Programming Perl 3rd Edition (Wall, Christiansen & Orwant)

Appendix

Platform support for Perl

Windows, Solaris, Linux, MacOS classic,

Acorn, AIX, Amiga, Apple, Atari, AtheOS, BeOS, BSD, BSD/OS, Coherent, Compaq, Concurrent, Cygwin, DEC OSF/1, DG/UX, Digital, Digital UNIX, DYNIX/ptx, Embedix, EMC, EPOC, FreeBSD, Fujitsu-Siemens, Guardian, HP, HP-UX, IBM, IRIX, Japanese, JPerl, Linux, LynxOS, Mac OS Classic, Mac OSX, MachTen, MinGW, Minix, MiNT, MPE/iX, MS-DOS, MVS, NetBSD, NetWare, NEWS-OS, NextStep, NonStop, NonStop-UX, Novell, ODT, Open UNIX, OpenBSD, OpenVMS, OS/2, OS/390, OS/400, OSF/1, OSR, Plan 9, Pocket PC, PowerMAX, Psion, QNX, Reliant UNIX, RISCOS, SCO, Sequent, SGI, Sharp, Siemens, SINIX, Solaris, SONY, Stratus, Sun, Symbian, Tandem, Tru64, U/WIN, Ultrix, UNIX, Unixware, VMS, VOS, Win32, WinCE, Windows 3.1, Windows 95/98/Me/NT/2000/XP and z/OS.

According to CPAN (the Perl archive) there are no ports for Inferno, OS1100, PalmOS, PRIMOS and VxWorks.

I can't find out whether ICL VME is included or not (I suspect not).

Links

www.linux-mag.com/1999-10/uncultured_01.html
perl.apache.org/
perl.oreilly.com/news/success_stories.html
use.perl.org/
www.activestate.com/
www.cpan.org/
www.perl.com/
www.perl.org/
www.perlarchive.com/
www.perldoc.com/
www.perlmonks.org/
www.scriptarchive.com/
www.tpj.com/
www.bbc.co.uk/education/betsie/download.html

Newsgroups

comp.lang.perl.misc
comp.lang.perl.moderated

Alex Brewer is Deputy Chairman of IRMA

Operational Risk Systems –

The fast Track to Achieving Compliance and Reducing Fraud

Steve Semenzato

Fraud is a far greater risk than banks have been prepared to admit, according to data compiled by Aon, the insurance company.

The average size of internal frauds reported by banks in Basel QIS3 was $300,000, and $68,000 for external frauds. The Aon database finds the average to be $3 million and $1 million respectively.

Risk *Matthew Crabbe* November 2003 Vol 16 / No 11

Systems in a Changing World

How do you build a system if you don't know what that system is supposed to do? This is the problem facing technology managers at large financial institutions preparing for the implementation of Basel II.

Part of the problem is that Basel II seeks improvements in process monitoring and control in order to reduce errors and fraud. This requires more than just data collection and analysis. It calls for close integration of people, process and technology, particularly in the middle layers (2,3 and 4) of the operational risk pyramid.

In a stable world these objectives would be challenging. But business is dynamic, straddling many countries and changing regulations. Some processes are mature and stable; others are constantly evolving.

Where business is mature, central systemised solutions can meet the challenges of operational risk. But where business is still evolving it is difficult to define system specifications – with consequent problems for the integration of information that must be jointly drawn from both environments. After all, a global counterparty position must include all exposure.

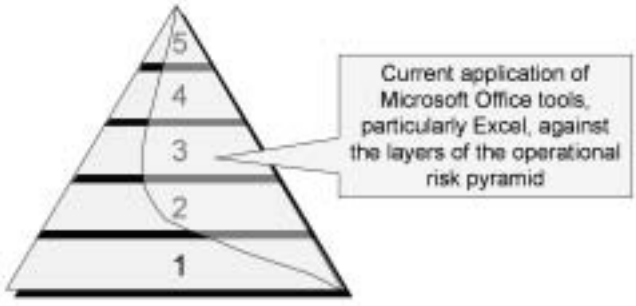
For many the response to these demands is one of delay i.e. "wait until there is clarity about what information should be gathered and where the rewards will come – give me the business case!". Yet, at a high level, the reward side of the business case is clear – better business understanding, reduced errors and fraud and a reduced capital charge. Can the log-jam be broken?

Build on the Business Investment, Don't Replace It

One answer lies in the fact that business is not waiting anyway. It is already moving forward, using those tools that are always at its fingertips – typically desktop solutions such as Excel, Access and Word.

In practice, Excel has become the most ubiquitous (though manually intensive) enterprise application integration tool in financial businesses. Data is drawn in large quantities from central systems and external data feeds. This is dropped into Excel and supplemented by manual entry for analysis and reports. A map of usage against the operational risk pyramid often looks like this:

Operational processes (Layer 1) are dominated by high-volume tools such as straight-through processing systems and



electronic confirmation matching. Control and risk self-assessment (Layer 2) calls for a combination of quantitative and qualitative analysis reporting that is ideally suited to desktop tools such as Word, Excel and Access. Equally, Excel-based reports dominate key risk indicators (Layer 3) and the collection of loss data (Level 4) and play a significant role in analysis (Layer 5).

The dominance of desktop tools in the higher layers is not surprising. They are flexible and their ubiquity breeds familiarity. Any professional can structure them to meet evolving business needs. This raises a key question – rather than seeking a replacement solution, why not continue to use them but resolve their weaknesses.

The weaknesses of desktop tools are well known – and are, ironically, a cause of operational risk themselves. What is needed to establish control?

- **Visibility** of the landscape of business-critical desktop documents and their links to data and reports, delivering clarity over data sources and dependencies and complete business intelligence.
- **Auditability** to see where, when and by whom changes were made to desktop documents
- **Security** The distributed nature and personalisation of desktop documents creates a security nightmare. With centralised monitoring everyone could sleep a lot more easily at night.
- **No Change in User Experience** is a vital element of any solution – Any solution that brings control at the expense of flexibility is doomed as the business moves forward.

Meeting the Demands of Basel II with Fast, Cheap, Agile Systems

These objectives are now achievable. Using a new data framework a full temporal history of desktop activity can now be available, capturing and structuring all changes in data, calculations and functionality, allowing distributed desktop data and applications to create a full system of record.

Systems establishment and evolution at the speed of the business is now possible. In particular for Basel II, such a framework provides:

i. Data collection and consolidation

Existing user-defined semantics and structures within spreadsheets are used to populate a SQL database, making it fully adaptable to the evolving requirements of the business. Since all data is captured, as soon as a new parameter can be captured or calculated in a spreadsheet it can become part of the real-time enterprise infrastructure. All the numerous complex data involved in credit and operational risk management can be captured, aggregated, evaluated and acted upon under a consistent corporate policy.

A key part of data collection is ensuring integrity and accuracy of that data. A framework that ties in all changes in desktop documents allows alerts to be linked to any aspect of the data or user activity, including additions, changes or abnormal behaviour. The flow of information can be tracked all the way through the enterprise to close data enquires rapidly.

ii. Reporting

Improved transparency from a range of reports is part of Pillar III of Basel II. With a complete history available, full trend analysis and monitoring of all key performance indicators contained in desktop documents is now possible. These reports can be delivered as standard web pages with rapid, cheap updates for new business requirements.

Ad hoc queries are easily performed. Should any parameter give cause for concern the database allows all precedent contributions to be analysed (including data, functionality, timing, document and author/user), right down to the level of forensic audit.

iii. Global real-time infrastructure

Full consolidation of enterprise data requires a framework that extends to all products and locations. No other approach can hope to deliver intra-day compliance for metrics such as credit risk.

With a wide variety of central systems, expensive and lengthy enterprise application modification and integration would normally be required. In contrast, the use of Excel (a global industry standard that is already holding much of the relevant information) in combination with a monitoring framework provides an immediate robust integration tier, substantially mitigating risk prior to considering much more expensive solutions.

The delivery of information via web-based portal pages (directly, or through the spreadsheets themselves) means that reports can be provided at speed across the entire business with negligible training or installation costs.

A Better Place to Start

Besides driving lower capital requirements, increased operational efficiency and increased transparency, the use of desktop applications and a data framework has several advantages over a traditional approach to systems implementation:

- Much faster implementation (days rather than years) leading to immediate benefits as existing business logic is utilised
- No business process change is required although, once in place, the platform offers many opportunities for evolutionary improvement.
- Users keep all of their existing spreadsheets, databases and other documents thus retaining the high productivity of business users and maintaining the high flexibility of the business.
- No end-user retraining
- Much lower costs
- Provides a single data repository for all desktop data, suitable for data warehousing or a single interface to an MIS system.
- Dramatically reduced time to trace errors in the data processing chain
- No expensive customisation of core infrastructure

For those looking to start the conquer of operational risk this must be good news.

Steve Semenzato is a director of ClusterSeven Ltd., and can be contacted at ssemenzato@clusterseven.com.

Case Chronology Best Practices

Greg Krehel

(This is the first of a series of articles which will deal with best practice in compiling information required for civil or criminal litigation. The best practices described are equally relevant to the audit process. In this article Greg explains the basics of getting your case into chronological order – Ed)

A fact chronology can be a tremendous asset as you prepare a case for trial. Yet, the majority of chronologies fail to live up to their full potential. Here are some simple steps that will help you get the most out of yours. From the starting gate to the finish line, assembling case facts in an accessible format can put you on track to courtroom victory.

The advantages are numerous. Chronologies are thinking tools. The very act of getting facts down on paper or in your computer clarifies thinking and makes the story of the case clear. Chronologies help ensure complete discovery. Which facts are disputed? Which still need sources that will be acceptable in court? And a chronology is a communication aid. A good chronology makes it easy for everyone on the trial team to share case knowledge.

Chronologies can also be used in a myriad of concrete ways. Use them when preparing for depositions, when developing motions for summary judgment and pretrial motions, in settlement conferences, and during trial.

Despite such benefits, during 15 years of jury research work, I've consulted on many cases where the effort to create a case chronology was abandoned during the discovery process. Why? In almost all these instances, work on the chronology ceased because the word processing document containing it became an unwieldy epic. There was no way to isolate facts of particular interest or view them in meaningful relationships. When litigators needed reports showing just the facts relating to specific issues, for example, they were stymied because of the all or nothing nature of word processing software.

Many litigators throw up their hands and attempt to memorize the facts or to jot them on legal pads. But this strategy invites disaster. Even the simplest of cases contains more facts than an attorney can keep in mind or organize meaningfully on paper. It's unrealistic to expect anyone to track notes scattered across many legal pads, much less to memorize 100 critical facts from each of 20 cases. When an opponent is using modern technology to organize and explore case information, the litigator with a paper system is operating under a dangerous handicap.

Unfortunately, those litigators who do stick with the task of creating a chronology often end up with unsatisfactory results. Many times, they end up with a list of case documents, sorted by date. Well, a document index is certainly useful when you need to get a piece of paper pronto. But it's hardly a chronology of case facts. Still other trial teams focus on facts, not documents, but create chronologies that contain just two or three columns: date, fact, and (sometimes) source. These layouts are a start, but they fail to capture critical information about the facts, information that can make the chronology far more valuable.

What's the solution? In the course of conducting jury research work on more than 300 civil and criminal cases, I've had the chance to work with and compare hundreds of case chronologies. Based on this experience, I have developed the following set of chronology best practices.

Don't Wait

Start a chronology as soon as you hear from a client.

From your first conversation with a prospective client, you're gaining critical knowledge about the problem that led the individual or corporation to seek counsel. You should begin to create the case chronology immediately upon returning from your first client meeting.

No matter how early you are in the case, and no matter how "small" the case may seem, as soon as your client has given you an overview of the dispute, you have been told more facts than you can easily memorize and manipulate in your head. And why even try? Your mind should be reserved for thinking, not memorization. Memorization is a job for your software.

If you start your chronology immediately, it can be used to good effect very early in the case. Take copies of the initial chronology to your second client meeting, and use them to clear up any misconceptions. Do the facts listed accurately reflect your client's understanding of the case? Can your client supply any missing dates? Can your client indicate which potential witnesses and what documents might be sources for these facts? Use the chronology also to focus your client on potential sins of omission. Is your client aware of any particularly favourable or unfavourable facts that don't appear in the chronology?

DB, Not WP

Use database software, not word processing software, to create your chronology.

In contrast to word processing software, database software makes it easy to create and maintain your chronology. If you employ a multi-user database, several trial team members can simultaneously enter, edit, and explore the facts. Database software automatically sorts your facts into proper date order. It can automatically provide the day of the week for each date you enter, and allows you to enter information using "pick lists," saving input time and eliminating the inevitable misspellings that occur with manual entry. And a database package can also automatically stamp each fact with the name of the individual entering it and the date and time when the fact was entered.

While the data entry advantages of database software are significant, its most important benefit is to make exploring your chronology far easier. When you print your word processing chronology, your choices are essentially all or nothing. You print the entire chronology or you don't print it at all. Thus, as your word processing chronology grows, it becomes increasingly unwieldy and diminishes in value.

In contrast, database software makes it easy to filter chronologies down to any subset of interest. Rather than printing a chronology that lists every case fact, print ones that contain just those facts that are particularly important, that bear on a particular case issue, that mention a particular witness, that are particularly good or bad, that come from a particular source document, or that others entered into the chronology while you were in trial on another matter.

List Facts, Not Documents

A document index doesn't pass muster as a fact chronology.

Many of the "chronologies" I've seen are really document indexes sorted by the date. While a document index is a great tool for managing documents, it is a poor substitute for a chronology of case facts.

Documents can be the subjects of facts, e.g., "The contract was signed on 5/10/99." And they can be sources of facts, e.g., Internal Memo #2 is the source of fact "Construction of Hyde Memorial Hospital began on 08/02/99." But documents are not facts in and of themselves. Therefore a document index, a listing of documents, does not pass muster as a fact chronology. A document index organizes knowledge by document rather than by fact. This approach ends up concealing facts rather than achieving the primary goal of a chronology, making case facts explicit.

A document index organizes knowledge by document rather than by fact. This approach ends up concealing facts rather than achieving the primary goal of a chronology – making case facts explicit. Documents, especially the important ones, are frequently the source of multiple facts. If the document chronology lists the name of the document, its author, recipients, etc., the facts it contains are never made clear. Including a summary of each document in the document index is not much of an improvement. Facts that may have occurred over a span of years are trapped in a single summary. It's up to you to read all the summaries and somehow pull the facts described in them into the proper chronological order. Here's the solution: Read each document and cull the critical facts from it. Enter these facts as a series of discrete items in your chronology. For each fact sourced from a document, enter the document's name or starting Bates # in the chronology's Source(s) column. Consider entering a page and line reference also.

When you take this approach, the facts found in each document will be listed at the proper point in the overall story of the case, rather than being trapped within a document summary. And anytime you want to get a summary of the facts found in a particular document, you can quickly filter the chronology down to facts coming from that source.

Define Fact Broadly

Include prospective facts and disputed facts in your chronology.

Some chronologies exclude facts for which a court acceptable source has yet to be developed. Others exclude facts that are disputed. Both tactics are a mistake.

If you don't enter a fact into your chronology because it's disputed or because you have yet to develop a court acceptable source for it, what's the result? First, you're turning yourself from a thinker of immeasurable value into a cheap disk drive. You end up having to memorize all these prospective facts. Second, you're losing an important benefit of your chronology — helping focus your discovery efforts. Facts without court acceptable sources are opportunities. Capture these potential facts in your chronology, and brainstorm about the witnesses and documents that might prove to be sources. List the probable sources in your chronology's Source(s) column. Then put your chronology to work. For example, when you prepare for a witness's deposition, filter the chronology down to those facts you were hoping to source from this individual, and develop a line of questioning that will elicit the facts in response.

Limiting the type of facts that are entered in a chronology is a vestige of using word processing software to create chrons. With a word processor, once a disputed fact or a fact without a source has been entered, there's no convenient way to get it out of your report when you want a pristine list of undisputed facts for use with motions for summary judgment and pretrial motions. However, if you're following my advice to create your chronology using database software, limiting your report to just undisputed facts or just facts that have sources is simply a matter of filtering your chronology using these criteria.

Here's another type of fact you should be sure to get into your chron: facts for which dates are inappropriate (e.g., the statement "smoking causes cancer" is a fact — though a disputed one — for which a date value is inappropriate). The term "chronology" suggests one should include only those facts that have associated dates. Don't let semantics restrict your thinking. A good chronology is much more than a diary of events. It is really a knowledge base of facts. All critical facts, including those for which dates are not applicable, should be included. (When you list facts for which a date value is inappropriate, consider entering "Not Applicable" or "N/A" as the value in the Date column. Thus, when you sort the chronology, all facts for which a date is inappropriate will be grouped together.)

Get Stupid

Move everything you know about a fact and its implications from your head into the chronology.

When you enter a fact into your chronology, make sure you get stupid about it. In other words, empty your head of all knowledge regarding it. Your chronology should be a memory replacement, not a memory jogger. If you don't get the complete fact into the chronology, you fail to clear your head of the minutiae so that you can focus on thinking. And you derail the communication benefits chronologies offer. If a critical part of the meaning of the fact is still hidden in your head, others on the trial team won't know about it when they read the chronology.

Every time you enter a fact into your chronology, pause and read it before you continue. Put yourself in the shoes of someone who doesn't know the case – say a new member of the trial team reading the chronology for the first time. Does what you've written represent your total knowledge regarding the fact? If not, edit the fact. While you're at it, ask yourself, "So what?" Does what you've written make the implications of the fact clear? If not, edit the fact. Further, if there isn't much of an answer to the So What question, give the fact a good once over, and make sure it belongs in the chronology in the first place.

Make Deposition Summaries Obsolete

Use your chronology in lieu of separate deposition summaries.

When you create a deposition summary, you're digesting the deposition down to its critical elements, i.e., to the critical facts found in it. If you follow the traditional path of creating a series of separate deposition summaries, the result is unsatisfactory. You end up with a separate story for each witness, rather than one complete story interlacing the facts found in various depositions and in other sources.

Stop creating deposition summaries, and use your chronology instead. Enter into your chronology the critical facts you develop from reading a deposition. In the chronology's Source(s) column, list the deposition's name, as well as the

volume, page and line number where the fact was found. Anytime you want a summary of a particular witness's deposition, filter the chronology down to just those facts that were sourced from a particular deposition.

Even if you use transcript search software, you should still enter in your chronology the key facts that occur to you as you read the deposition online. Transcript search software makes it easy to find the needles in the haystack of deposition transcripts and document OCR text files. However, once you find a needle, doesn't it make sense to get it out of the haystack?

You may have other documents besides deposition summaries where you're storing facts. Consider replacing all of these separate containers with your one master chronology. Instead of searching multiple places for critical case knowledge, you will always have the case facts at your fingertips.

Avoid the AKA Headache

Refer to one person, organization, or document by one name.

Want to filter your chronology down to just those facts about a particular witness, organization or document? Even if you're using a database program to develop your chronology, you've got a big problem if the same thing is referenced by different names. You first have to identify all of the different name permutations. Then you have to create a compound query that will find any fact that contains one of these possibilities. What should be accomplished in an instant becomes an hour long chore.

It's easy to end up with inconsistent naming. Suppose you're working up a medical malpractice case that involves Hyde Memorial Hospital. Unless you're careful, you're likely to have facts that refer to Hyde, Hyde Memorial, HMH, HM Hospital, and Hyde Memorial Hospital, among other possible variations.

The solution: develop a cast of characters list and establish a single alias or nickname to be used for each key player in the case. Typically, it makes sense to pick something short (e.g., for Hyde Memorial Hospital, HMH is probably the best choice). If you do, you save keystrokes in addition to gaining consistency.

Distribute the cast of characters report to the trial team. Ask that everyone working on the chronology use this dictionary if they are unsure of the proper name to use for a particular person, organization, or document. Naming consistency requires a little more work up front, but it quickly delivers a handsome return.

Use Fuzzy Dates

If possible, substitute question marks for portions of a date of which you're unsure.

As you build a chronology, you'll find yourself with many facts for which you have incomplete date information. For example, you may know that a meeting took place in March of 1999, but have no idea as to the day within March. Or you may know that a contract was signed sometime in 1998, but have no idea of the month or day. And you may know the accident took place in the 7 o'clock hour, but not know the minute or second.

What's the best way to deal with this problem when entering dates? Make it your practice to substitute a question mark for the portion of the date or time of which you're unsure. Using this simple tactic: March of 1999 becomes ?/3/99, sometime in 1998 becomes ?/?/98, and sometime in the 7 o'clock hour becomes 7:??.

We call this practice "fuzzy dating." Fuzzy dating allows you to capture what you do know about a date and makes what you don't know explicit. Fuzzy dating makes it easy to identify facts needing date research. When you obtain better information, you can return to the fact and update its date and time value.

Fuzzy dating is effective if you're working up your chronology in a word processor or with some litigation specific database packages. However, many database packages do not permit you to enter any date value other than a complete one.

Off the shelf database products are designed for generalized use and not with the realities of litigation in mind. These products attempt to help you by validating your date entry. Unfortunately, these validation routines backfire when you don't know the complete date. Enter ?/3/99 into a date field in Microsoft® Access® , and it will give you an error message every time. If the database software you're using only supports complete dates, you have at least a couple of alternatives: (1) When you don't have complete date information, you can leave the date cell blank and (2) You can assign an approximate complete date (e.g., the fact we know happened sometime in March could be dated 1/3/99). Both solutions have obvious downsides. The lesser of evils depends on your circumstances.

Indicate Disputed Status

Each fact should be flagged as being disputed or undisputed.

I've already argued that your chronology should include disputed facts. If your chronology contains a mixture of disputed and undisputed items, it makes good sense to create a column which indicates whether a given fact is undisputed or disputed, and if so, by which party. Consider titling your column Disputed Status and using these values: Disputed by Opposition, Disputed by Us, Undisputed, Unsure. (If you're working on a case with more than two parties, revise the options to whatever you deem appropriate, however, you will probably find that having an option for all possible permutations is overkill.)

Once you've marked facts as being disputed or undisputed, your chronology becomes a tremendous aid in the preparation of motions for summary judgment and pretrial motions. For example, instead of creating a last minute list of facts to which you are willing to stipulate, you simply filter your chronology down to the undisputed items and print. If you've begun your chronology early in case preparation, you can use this information to organize your examination of adverse witnesses. Filter the chronology down to those items that you expect to be disputed and see if you can obtain admissions regarding them during depositions or find sources for them in documents.

Show Issue Relationships

To create a great chronology, you need issues as well as facts.

The vast majority of cases involve multiple issues. Assessing the strength or weakness of your case is really an exercise in assessing your strength or weakness in relation to each of the issues in it. Here again, your chronology should be an important aid.

Develop a list of case issues (perhaps with the aid of a brainstorming session if you're one member of a trial team). Don't limit your thinking to those issues tied directly to some legal claim. Include any topic that might influence juror thinking. For example, if you are working for the defense in a products case, you might want to include this issue: The Plaintiff Is Motivated by Greed, Not a Desire for Justice. Even though you

would never make such an argument explicitly, it would be interesting to see what facts point to plaintiff greed, allowing jurors to reach such a conclusion on their own.

Now add another column to your chronology: Related Issues. In this column, name the issue or issues on which each fact bears. You can capture issue relationships as you first enter the facts. Another alternative is to forego entering this information initially and ripple through the chronology at a later point focusing on issue analysis. Establishing relationships between facts and issues is also a logical place to parse work among members of the trial team. Junior members of the team can cull facts from documents and depositions. Senior members of the team can make links between facts and issues. Creating links between facts and issues makes it easy to print chronologies of just those facts that relate to a particular issue – a capability that has great value when you analyze your case and develop your strategy.

Take An Issue Driven Approach

Use your issue list to ensure you have a complete chronology and to generate a fact "wish list."

As you develop your chronology, consider taking a "top down" or "issue driven" approach to your case. As case preparation begins, and one or two times a year thereafter, conduct a brainstorming session in which you think about your facts on an issue by issue basis.

Prepare by printing for each issue a mini-chronology of the facts that bear on it. Begin the brainstorming session by reviewing the chronology of facts related to the first issue in your issue list. Then set the list of facts aside, and think about other facts of which you're aware that bear on this issue. Enter these additional items into your chron. Next, think about the facts you wish you had for this issue. If you think there's any chance of developing such a fact, enter it in the chronology and list any potential sources that come to mind. Repeat this process for each issue in the case.

In the early days of a case, this issue driven brainstorming process can be an invaluable aid in organizing discovery. As the case matures, it becomes a great way to reflect on case strengths and weaknesses and develop strategies in light of them.

Evaluate Each Fact

Separate the sheep facts from the goat facts.

Not all facts are created equal. Some are critical; others are trivial. Some are great; and, unfortunately, others stink. To get the most out of your chronology, you should rate each fact in terms of criticality and goodness/badness. Once this is done, you can filter the chronology down from all facts to just those facts that are critical or just those facts that are particularly good or bad.

One solution is to use two columns to capture evaluation information: one for criticality and another for goodness v. badness. A simpler method is to fuse both criticality and goodness/badness criteria into a single scale. For example, if you're using database software, you could create a pick list with the following values: Heavily For Us, For Us, Neutral, Against Us, Heavily Against Us. When you evaluate something as being heavily for you or heavily against you, you are indicating that it is critical. (The downside of the single scale solution is that it makes it difficult to evaluate those facts that are critical but are neutral in terms of goodness/ badness. However, the reduced work of the single column probably outweighs this shortcoming.)

If multiple litigators are collaborating on a case, consider creating an evaluation column for each. Each individual can make their own assessment, and your software can isolate those facts where evaluations vary widely.

If you want, you can skip evaluating facts when you're first entering them into the chronology. Later, at an appropriate point, ripple through the chronology and evaluate the facts in one sweep. Here is another place where the work of maintaining the chronology can be distributed to various members of the trial team. Junior members of the team can enter the facts. Senior members of the team can evaluate them.

Put Your Chronology to Work

Use your case chronology in practical ways.

Your chronology should be far more than a thinking tool. It should be a practical aid in communicating about your case with your client, the opposition, and the trier of fact.

Use your chronology to communicate with your client. Send your client the chronology on a regular basis, perhaps quarterly. If you are using database software that stamps each fact with the date when it's entered into the chronology, have the software mark with an icon each fact that was entered since you last sent your client the chronology. By tagging new facts in this way, the report will give your client the complete story of the case, but it will be easy for them to focus on the new evidence.

Use your chronology at settlement conferences. Show opposition counsel and their client why the facts back your view of the case. Show them that you're organized and will be a formidable opponent if they choose to be unreasonable. (Obviously, before you print your chronology for use during a settlement conference, you'll hide columns such as Evaluation.)

Use your chronology to make a powerful case to judge and jury. Chronologies are great tools for educating the jury during opening statement and for illustrating your arguments during closing.

You can even use chronologies to expedite the development of your new associates' case analysis skills. The day they arrive at the firm, assign each new associate to one or more cases, and make them responsible for developing a chronology for each. At set intervals (once a month?), have each associate submit a chronology that contains just the new facts they have entered. Critique the verbiage used to describe each fact, their determination of whether the fact is disputed or undisputed, their evaluation, and their analysis of the issues on which the fact bears.

Summary

A chronology has the potential to be a tremendous aid as you organize and explore case knowledge. If you adopt the practices outlined above, I believe you'll realize this potential in full. I would appreciate your feedback.

Greg Krehel is CEO of DecisionQuest's CaseSoft division (www.casesoft.com). He can be contaced at gkrehel@casesoft.com.

E-mail Archiving: A Vaccination Against Regulatory and Legal Distress

Priscilla Emery

E-mail: The New "Smoking Gun"

A recent study by the *META Group* points out that e-mail has become the preferred communication tool for business executives. This pervasive business tool has created new challenges for IT network managers, records managers and legal departments in many organisations. In addition to the impact that the increase in e-mail volume has had on storage requirements for e-mail administrators (you know it's growing – just look at your own in-box), the ways in which e-mail have been used by the business community are causing organisations to view "managing" e-mail as more than just an exercise in conserving storage resources.

One first has to look at the position that e-mail is taking in the overall enterprise repository of information to better understand its impact (see Figure 1). If you look at where e-mail sits in this diagram it fits squarely in the Document space and it has become a very crucial document, not just in terms of transferring information from one person to another, but sometimes serving as an historical record of a business transaction. You can see that not all documents or data elements are records but records can take the form of any number of different delivery and format mechanisms, e-mail being one of them.

This mix of potential delivery mechanisms coupled with new regulatory issues associated with retaining corporate information is causing a widespread interest in how to effectively manage not just e-documents but e-mail in particular.

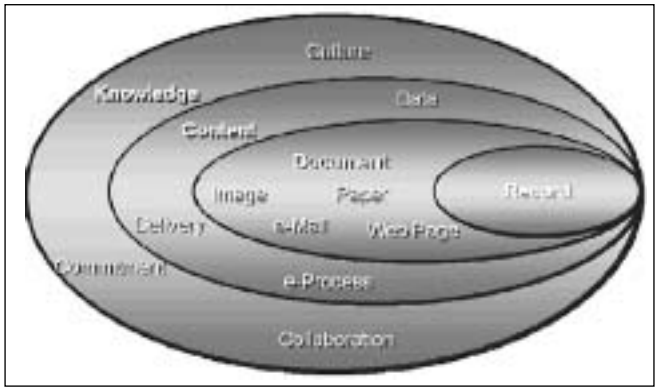


Figure 1: e-Nterprise Repository Source: e-Nterprise Advisors

Headline grabbing events such as the shredding of evidence at Enron; the e-mail trail of conflict of interest at Merrill Lynch, Citicorp's Smith Barney and other financial investment firms; and even the U.S. Department of Justice vs. Microsoft case have proven just how crucial e-mails can be in the document trail of evidence. As a result of those events government regulators have become significantly tougher about making sure all communications that occur during the course of providing financial data to shareholders and other public entities are reproducible in an audit or investigation. E-mail has become the "smoking gun" in many of these investigations and has also become a "lightning rod" of attention for auditors and lawyers alike.

Although the Sarbanes-Oxley Act of 2002 outlines a variety of different activities that now must be supported by public companies, such as having truly independent audit committees, the bottom line of this act is that all of these communications need to be archived for a specified length of time and immediately recoverable and reproducible on request by shareholders, auditors or regulatory agencies. The underlying assumption is that if the document or e-mail cannot be produced when requested there must be an intent to defraud or to circumvent the system, which consequently involves some serious financial penalties and potential jail time.

Still, there have always been negative consequences for using e-mail to participate in what may be viewed as unethical or illegal conduct — that hasn't changed. Several financial services companies have been slapped with significant fines over the last several years for conflict of interest activities that have come to light through the investigation and eventual recovery of e-mail-based documents. E-mail has been heavily used as evidence in the recent Credit Suisse First Boston investigations, where Mr. Frank Quattrone has been charged with allegedly telling his employees to delete e-mails and other potential evidence just prior to a government investigation.

E-mail is a prime target of evidence in many litigation activities these days and that activity continues to increase. Sexual harassment claims and suits subject to potential private litigation rely even more on e-mail-based evidence as well. And with the Sarbanes-Oxley act providing an outlet for shareholder grievances, the rate of shareholder lawsuits to recover lost investments will probably not reduce this trend.

The cost of attempting to deal with these types of lawsuits can be astronomical (whether or not the company is at fault). For example, American Home Product's Wyeth-Ayerst Pharmaceutical Division became the subject of a lawsuit in Massachusetts related to its "Fen-Phen" diet drug. It was claimed that Wyeth-Ayerst had known that Fen-Phen produced some serious contra-indications for some patients but had failed to disclose this knowledge to physicians and the public.

The deposition process required that the Company recover the e-mail of about 15 employees from more than 800 back-up tapes. The defendants estimated the cost of restoring the tapes for electronic discovery would cost anywhere from $1.1 million to $1.7 million. Wyeth-Ayerst chose to settle out of court so it may not have had to incur those particular costs but guilty or not, it remains an expensive proposition to defend any company when e-mail-based documents are required as part of the deposition process.

Why Is E-mail So Troublesome?

It doesn't help that e-mail can be a "troublesome" document and/or record to actually manage. E-mail systems allow messages to be changed before forwarding so that the "original" is not what it seems to be to the receiver making it imperative that e-mail records be "locked" before being retransmitted. Annotated items and comments can also be

deleted that may be crucial to the record of a transaction. E-mail systems also allow for indirect addressing through distribution lists, and blind copies, making it difficult to track whether or not someone who is NOT really supposed to have access to the information is being included. E-mail messages can contain embedded links that can take a reader to an information item that exists (or at least used to exist) elsewhere.

And the most troubling problem – most users keep hundreds of old messages on their desktops and on their personal folders on e-mail servers. As the number of daily messages grows, and those messages increase in size, organisations may see a growth in storage overhead of 100% to 150%. Storage of these messages is having an impact on overall e-mail server requirements. E-mail administrators are constantly asking e-mail users to delete unwanted or unnecessary messages so that e-mail servers can operate efficiently. Unfortunately, this request can be counterintuitive to the notion that e-mail should be saved as a record. The challenge for many organisations is to keep e-mail servers optimised for peak performance while at the same time making sure that the right e-mails are being archived (and/or deleted) at the appropriate time.

Mitigating Risk By Managing E-mail Assertively

Given all these potential threats, what can IT managers do to avoid the consequences of noncompliance or minimise the costs associated with potential litigation? Well, the one thing they can't do is nothing. Of course, sometimes doing "something" isn't really effective enough, such as doing daily back-ups of e-mail servers at the end of the day. A back-up file only provides a snapshot of what is still left in the e-mail server at the end of the day. A lot of e-mail that should have been archived for regulatory reasons could have been deleted during the course of the day. That e-mail will not show up on a back-up tape. And, even if it did end up on a back-up file, finding these un-indexed e-mails several months or years later would be very difficult. As a consequence, organisations should evaluate e-mail storage and archival alternatives to address this issue.

Before evaluating e-mail archiving alternatives it is very important to do some serious internal planning and answer some key questions that will impact your implementation approach.

Understanding what your organisation is trying to accomplish from a compliance standpoint goes a long way to understanding what types of internal procedures need to be developed and what tools need to be evaluated. For example, compliance with Sarbanes-Oxley is really focused on the use of archiving tools while compliance with HIPAA[1] may be focused on privacy tools along with archiving tools.

In all cases it is mandatory that appropriate policies and procedures be in place first. Most archiving tools only help to enforce or manage approaches already in place. For example, a file plan with record categories defined should already be in place before an organisation can effectively use an e-mail archive product for e-mail records management. No automated system (even ones that automatically index e-mails and records) can produce effective results if categories have not been defined prior to implementation.

That said, a secondary step to creating a policy is enforcing it and enforcing it consistently. Organisations that do not consistently enforce record keeping policies are subject to the same legal liability as those that don 't have any policies at all. In the case of enforcing record keeping standards, this involves a combination of training at appropriate levels of the organisation and timely quality assurance checks on record keeping practices. In the case of the misuse of e-mail (such as internal sexual harassment), perpetrators have to be actively admonished or expelled, as outlined in any internal policy, in a consistent way (i.e., the organisation cannot admonish one person but ignore someone else) or be subject to a potential lawsuit. Again this type of enforcement also involves providing training and the appropriate compliance checks. Many other issues still need to be sorted out when evaluating e-mail management tools and services.

- What part of the e-mail is being scanned for content, viruses, etc.? The Header? The body of the Message? The Attachments? All of the preceding? When it comes to archiving it may be sufficient to scan the Header if you use only standard headers for certain types of messages that have to be stored. This scenario is highly unlikely but every organisation needs to identify what types of e-mails need to be archived and figure out how to identify them as easily as possible.
- How intrusive is the product you plan to use? Not just to users but to the e-mail administrator as well. It should go without saying that adding new fields for users to classify and file e-mail, as either a record or other repository-based document, is additional work that most users will not welcome. Finding a system that aids in pre-population of file plans, and providing a familiar user interface (i.e. Microsoft Outlook, Lotus Notes, Internet Browser) will go a long way to making sure the product gets used appropriately. E-mail administrators already feel overworked and sufficiently challenged on a daily basis so that any new "management" tool should not add a significant amount of "overhead" to the e-mail server's storage needs and provide value-added reporting and tracking capabilities for the administrator.
- Is auto-categorisation or automatic indexing an option you want to consider? For knowledge gathering applications, auto-categorisation can be a useful tool to automatically file and categorise e-mails based on the content. These applications can be a little more fluid than more rigorous archival applications and although consistency is important, it is not as mandatory as in a record keeping system. Record keeping systems can also use auto-categorisation but it is recommended that a significant quality assurance testing and implementation effort be completed before rolling out the capability en masse. Auto-categorisation can enhance compliance efforts by making it easier and less time consuming for users to file all kinds of records including e-mails.
- How much customisation is required to implement the product in your environment? As we all know, customisation can run into a significant sum of money, especially if the product is completely incompatible with the normal procedures used in an organisation. In addition, integration with legacy systems must be taken into account.
- Is it easy to access and retrieve archived e-mails when required? Ease of access is a two-way street. On the one hand, people who have authorisation to access information should not have to wade through confusing interfaces and several layers of software to get to the e-mails needed. On the other hand, there should be sufficient security on the system to limit access to only those who should have it.

[1]Health Insurance Portability and Accountability Act of 1996

Another question related to this one is, what software do users need on their desktop for retrieval of archived e-mails? This could be asked of either software or service providers. If plug-ins are required on the desktop how will they be proliferated and how much time does it normally take for them to "boot-up" when needed?

- Can the tool handle all your e-mail servers? Many large companies have multiple e-mail products supported in-house as well as multiple e-mail server nodes. Many email archiving products support a variety of different e-mail systems but can these products support different systems at the same time? And, even if only one type of e-mail application is used, can the product or service handle traffic from multiple e-mail servers?
- All applications should address the question of what types of auditing and logging facilities are provided. How much overhead do they add to the system or to the service?
- Then there is the long-term plan of how to view these e-mails (and other stored records and attachments) after they've been archived over a long period of time. Will you still be able to read these e-mails and attachments after seven years (a virtual eternity in technology years)? Are the e-mails and attachments saved in a proprietary format? Is there an option or plan to copy e-mails to a non-revisable media such as optical disc for long-term preservation? Having a defined plan for either migration or long-term viewing is essential.
- If you are archiving for record keeping purposes is the product DoD 5015.2 certified? Certification doesn't guarantee that the product has all the records management functionality that you may require but it does help to know that the baseline requirements for handling meta-data are supported correctly. In addition, you should also be constantly aware of changes to the "standard" that may impact implementation efforts in the future.

If managing e-mail as a record is your primary objective some other functions and features must also be taken into consideration. The authenticity of the e-mail record has to be maintained and the e-mail has to be "unalterable" from creation to its final disposition.

In order for an e-mail record to be deemed as "usable evidence" it needs be prepared to be subject to legal scrutiny to overcome any legal objections during any potential court or discovery process. The following activities need to be supported:

- The capture of incoming and outgoing e-mail messages at time of creation or receipt
- Retention rules should be applied systematically
- Consistent application of a file plan with policies and retention schedules.

Record integrity also depends on three attributes: content, context, and structure. Therefore, moving a complete e-mail record and its attachments, optimally in native document format, out of mail servers may change content, context or structure or loss of e-mail metadata. Retention information should be integrated into message stores and/or repositories.

An Approach to Archiving E-mails

One of the leading software packages provides Plug-ins for Microsoft Outlook allowing a user to move their e-mail messages (including attachments) from the proprietary MS Outlook or Exchange data repository into an open source XML format.

It converts an e-mail message to one XML file (holding e-mail structure, address information and plain body text), one RTF file with the formatted body text (if present) and one XML wrapper plus the original file for-mat for every attachment. (See Figure 2). The screenshot in Figure 3 illustrates how this process looks to the user.

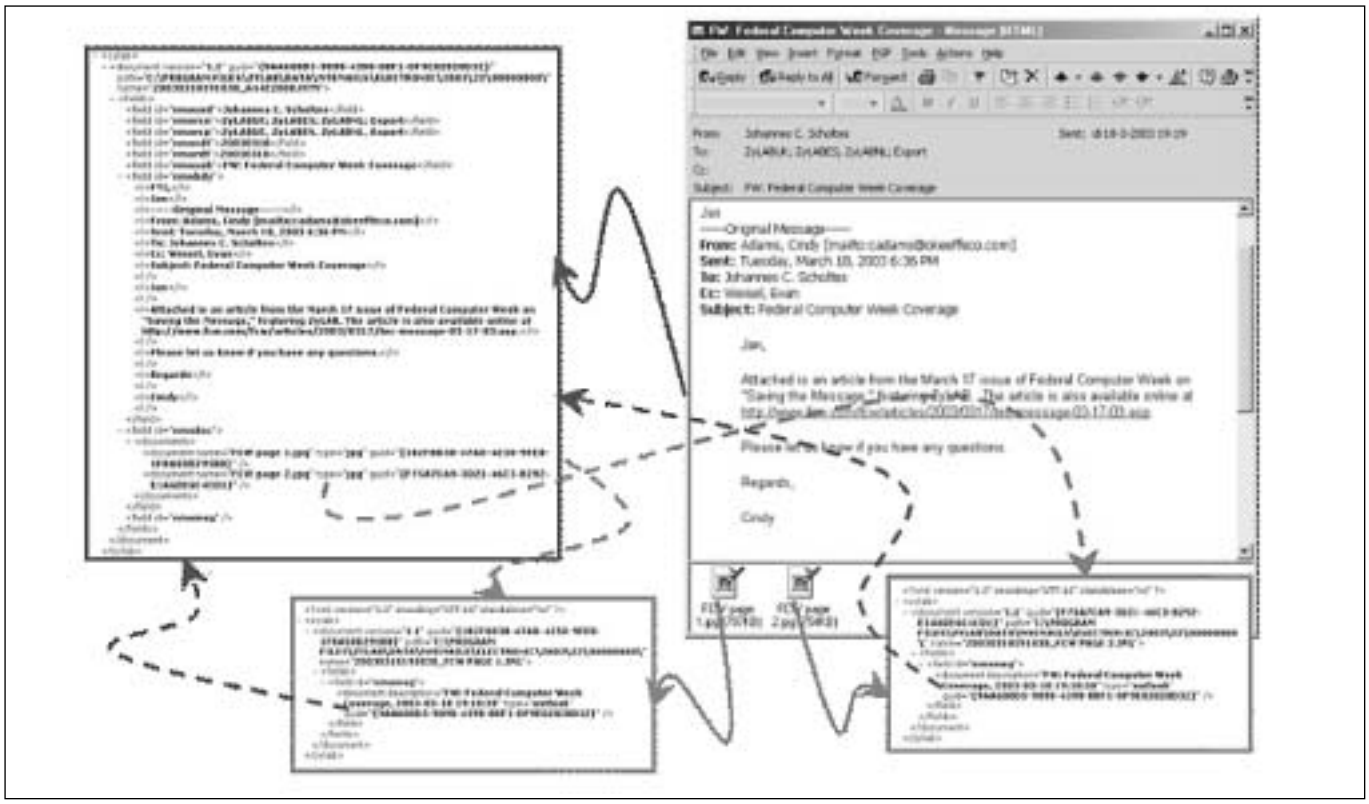


Figure 2: Converting MS Outlook e-mail to XML format

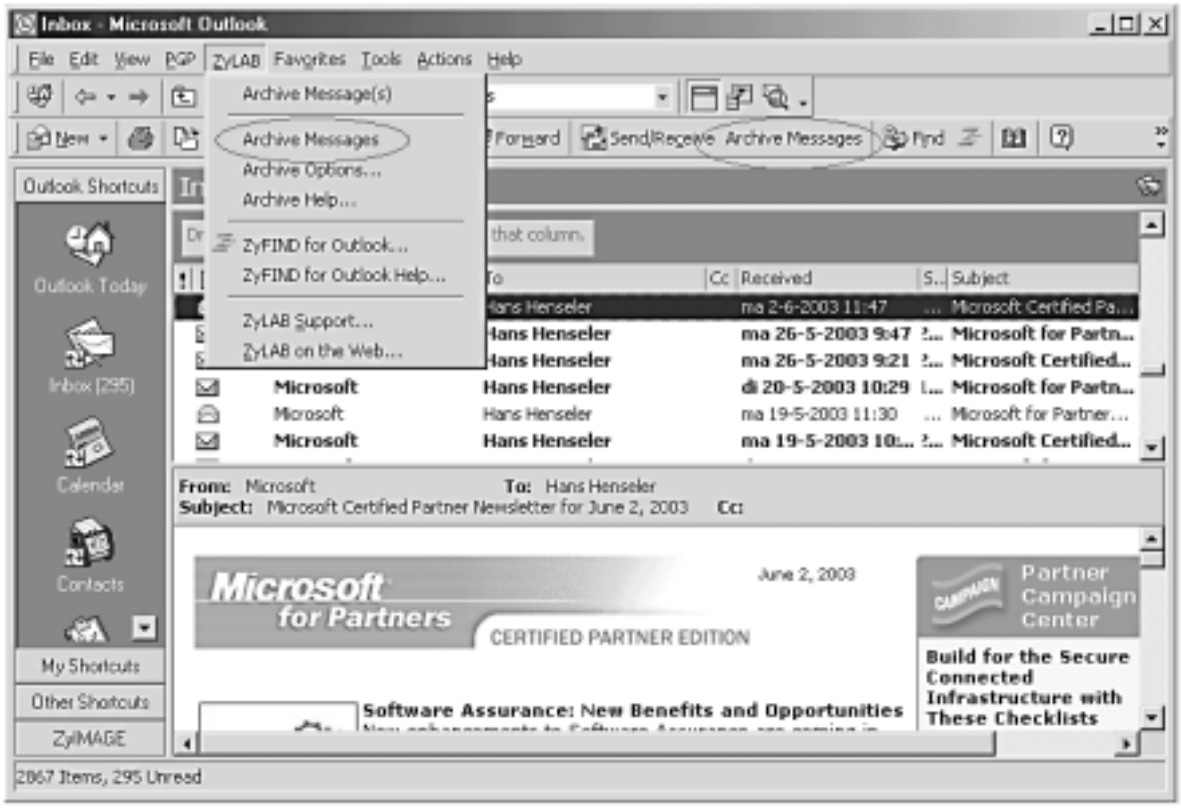


Figure 3: Archiving Plug-in for Microsoft Outlook

A user can open a message to access an attachment or open an attachment to access the associated message. Archived e-mails can be marked by adding some text to the SUBJECT line such as "archived on <date and time> in archive <x>." Simplicity is the key element here. In addition to being fully text searchable, records management functionality can be incorporated into the archive allowing for the storage and deletion of e-mails based on defined policies.

Managing E-mail: More Than Just a Regulatory Issue

The knowledge sharing aspects of managing e-mail should not be overlooked. An archive can also serve the purpose of making e-mails a part of overall corporate memory, and providing a way of accessing messages and attachments so that they can be found when needed.

According to a KPMG survey conducted in 2000, 60% of employees spend more than one hour per day duplicating the work of other employees. If the average professional employee costs an organisation at least £54,780 a year, employees spend roughly £6,850 duplicating work each year. That's a lot of productivity and money going down the drain.

One solution is to save all e-mails in a .pst file, index this repository and then search the entire repository when you need to find something. This approach is also useful for forensic investigations, corporate e-mail analysis and other knowledge e-based applications.

- A user can also search for information based on the meta information of the e-mail messages, or fields. These different field types include: Filename, Subject, Sender, Mailto and CC. The e-mail repository can be also searched.

Waiting Till You Are Investigated Is Not the Time To Implement!

The bottom line for e-mail archiving is that regulators, auditors and lawyers will not be sitting idly by waiting for your organisation to "get ready" to archive e-mails. They are moving forward with investigations and audit activities whether your systems are ready or not.

Remember: You Are Being Watched

…by the government
…by potential litigators
…customers
…hackers

Being proactive about archiving e-mail can mitigate risk and save £££'s

E-mail archiving should be viewed in much the same way as you may few getting your annual flu shot. You can take the chance that you won 't get the flu this year and not get a shot but if you do you may get lucky enough to catch it in time to treat it quickly or you could wind up being out sick for a week or two. The other alternative is get the shot and be prepared so you don't have to worry about getting sick and be productive throughout the season. If you don 't archive your e-mail systems quickly you are playing "Russian Roulette" with authorities and with your companies exposure to litigation. If you do implement e-mail archiving tools and practices you will at least be prepared for the attack and save time, money and resources in the long run.

Priscilla Emery is President and founder of e-Nterprise Advisors. She can be contacted at pemery@e-nterpriseadvisors.com

ZyLAB UK Limited
Is a leading provider of document imaging and paper filing software. For more information access www.zylab.com

Email Forensics

Clive Carmichael-Jones

Introduction to Email Forensics: Defining the problem

Not all that many years ago, it was possible to label yourself as an expert in computers and for this to be believed. Today no such illusion is possible, and the complex area of email forensics is a good example of why this is so. The issues that are raised by the application of forensic science to emails often are technically complex, and frequently legally challenging.

The email system of today's businesses must be considered as the corporate filing system and more; containing every bit as much information as a payroll system or other corporate database.

In addition to strategic corporate information, the modern email system may provide an insight into the love life of staff, their hobbies, holiday and career plans. It may be the route via which intellectual property leaves a business or viruses, worms and Trojans enter a system. It provides an historical record of what has happened, an account of what is currently happening, and a view of what is planned.

Modern systems are used by the majority, administered by the minority and understood by precious few. This applies both internally within an organisation and generally across law enforcement and computer investigation communities as a whole.

Mass media coverage of what is possible during an investigation ranges from (occasionally) reasonable, fair and considered, through to sensationalist and speculative. The public's perception of what is possible, and what is routinely achieved, is thus similarly broadly based.

The following sections will seek to look at some of the technical issues that may face an investigation team when electronic email systems form part of evidence, and briefly discuss some of the legal implications.

The scope of email technology

"It's so much easier to suggest solutions when you don't know too much about the problem."

Malcolm Forbes (1919 - 1990)

Before looking in any detail at some of the problems, one must first consider what is actually meant by the term 'email system'. This term is not as straightforward as it may seem, as it is now used to encompass a number of similar, but functionally different, technologies.

Broadly, email systems can be classified as being either web-based, or server-based. From the perspective of the forensic investigator, the nature of the case is determined by this basic distinction.

There are a whole range of other terms and acronyms frequently used and more frequently misused, to describe 'email'. Internet relay chat, peer-to-peer chat rooms, newsgroups and news servers are just some of the descriptions which can appear liberally scattered in various expert reports, papers, and statements.

Web-based email systems

Web-based email systems are accessed via a standard web browser. From the point of view of the user, it offers a number of benefits:

- Simplicity of use: the user does not need to understand how to set up a complex email system client, beyond entering a username and password. The email provider's site is viewed and a user-name and password is used to retrieve email. Many providers offer this as a free service, MSN hotmail being the most widely known of these. There are some disadvantages to most free services, in that they offer a relatively feature free service, and only a small amount of storage space is allocated to a single user. This is particularly restrictive if large email attachments are associated with an email. Typically if a user exceeds their allocated limit, the service provider may delete messages, and once deleted it is usually not possible to recover them. This has significant implications for the timeliness of an investigation, especially if it is anticipated that an investigation is likely to span many months, or perhaps even years.
- A high level of mobility and accessibility: because emails are accessed via a standard web browser, a user can view their emails at any point in the world that offers a connection to the Internet, whether hotel, airport, Internet café or home.

The real benefits to users of web-based email systems, mean that they are very popular outside of the corporate environment; these systems will also feature in a significant proportion of investigations, both civil and criminal.

Server-Based Email Systems

Server-based email systems are usually accessed via the standard Post Office Protocol version 3 (POP3), described under Request For Comment (RFC) 1725, or less frequently, the Internet Mail Access Protocol (IMAP) described under RFC 3501. For information regarding the relevance of these RFCs, see later.

No matter which protocol is used to access emails, a server-based mail system stores a user's email and attachments on a remote server. The user connects to the server using specialist email client software, for example Microsoft Outlook Express or Eudora, and the emails are downloaded to the user's local machine. After this transfer is complete, the email is deleted from the remote mail server. The server-based system is the one most often provided by an Internet Service Provider (ISP).

The email client software that provides access to email, will also afford a range of powerful facilities that are not generally available through web mail-based services. Examples of the sort of facilities offers are:

- the ability to create email aliases
- the ability to create email groups
- mailbox creation options
- advanced mail filing and searching options
- email forwarding facilities

It is possible to configure a web browser to access a POP mail account, and this is something that should be considered when

involved in an email related investigation, even within a corporate environment.

It is clear that most investigations involving large businesses or organisations will involve server-based email systems, often with the mail server residing on the business premises. This does not of course preclude the use of supplemental web-based systems. Indeed a number of investigations, especially those involving disaffected or disgruntled employees, involve the use of web-based systems in combination with server-based systems.

Sources of technical information

There are many sources of information that an investigation team can employ. Some will be provided by software developers of an email system under consideration, some by independent third parties. Some will be authoritative, others less so. One of the most useful sources of information is freely available online, and comes in the form of RFCs.

RFC documents are a series of technical and organisational notes about the way the Internet works. The Internet Engineering Task Force (IETF) and the Internet Engineering Steering Group (IESG) define the official specification documents. The published standards form what is effectively the 'manual of how things work' on the Internet.

The first RFC, RFC 1 relating to 'host software' was issued over 30 years ago, and there are now well over 3,600 RFCs. These tend to be by their very nature somewhat technical documents, but then email forensics when carried out at a low level, tends to be a somewhat technical process.

For example, those wishing to dabble in the area of reading and interpreting email headers, RFCs 1869 and 1870 are useful starting points. If you are curious how the Post Office Protocol version 3 (POP3) works, the RFC 1725 is a good beginning.

A word of caution: The reader should always start from the latest version (biggest number) of the RFCs. It would probably come as a disappointment to study and memorise an early RFC, only to learn that the standard had been revised several times and the text that had been carefully studied was obsolete. Equally, it is also worth considering the timeframe within which the data from an investigation is set. Quoting from standards that came into force after the event is not to be recommended.

Capturing the Evidence

This is the first step in an investigation, and a wrong decision made at this stage is likely to have serious consequences later. How should evidence that resides in an email system be captured, and what are the practical problems that may occur?

The answer to this question depends upon where the email data is physically located. When considering a web-based system, the first practical problem is one of locating the physical server, and determining the legal jurisdiction within which that data resides. Whilst this can seem a rather superficial problem, it is an aspect of an investigation that can often lead to the most significant problems.

It is relatively straightforward to narrow down, from the IP range of a server for example, the email data's likely geographical location. Success in actually securing the electronic evidence is often more do to with the skill and tenacity of the legal representation, rather than pure technological skill. Sad to say a little good luck is often helpful at this stage too.

It is fair to say that a majority of civil and criminal work involves server-based email systems. These too can offer a range of technical problems to keep investigators occupied, even without considering some of the wider legal implications.

So what technical factors must an investigation team consider when attempting to capture electronic evidence from an email system?

Asking a simple question illustrates how complex this seemingly straightforward problem can rapidly become:

- Where is the mail server?

  It is more than a little embarrassing to enter business premises, possibly under a search and seize order, or search warrant, to capture the information held on a corporate mail server to discover either: the mail server resides overseas in another regional office, or the mail system is outsourced to an Application Service Provider (ASP). This of course may also be located virtually anywhere on the planet.

  Having overcome the first major technical hurdle, that is to say finding the mail server, the next set of question must be asked (and answered):

- What is the next course of action?

  Assuming a server-based system, the strategy for collecting and investigating the tracked down emails should now be considered.

  a) Is it possible to image a mail server and all that this implies? That is to say, bring it down safely, image it, return the mail server to a working condition, and subsequently be able to deal with the image files to generate meaningful and evidentially safe, evidence. The imaging option does provide the most complete information regarding the email system, which will be discussed later.

  b) Is it possible to seize reliable, full backup tapes of the email system, or if they do not exist, is it possible to create a full backup set now? If the full backup tapes are accessible, is the relevant skill set available to be able to do anything meaningful with the tapes? There are consequences that the backup option will have on the system, but it does give the advantage that there is no requirement to bring the system down. Used in conjunction with an image copy of a system, this data can provide useful timeline information regarding the state of a system at varying points in time. The precise nature of an investigation has a significant bearing upon the relative weight and importance of such factors.

  c) Is it necessary or possible to conduct a live investigation on a system? Frequently this option is exercised, with the justification that it is the only reasonable way that an investigation could be progressed. Actually what is meant by this is the investigator did not have the technical ability or tools to fulfil either option a) or option b) above. There is very little justification for soundly trampling upon fundamental principles of reproducibility and auditability in this way. The defence for these actions normally given at this stage is that an investigator was competent to determine exactly the implications and consequences of their actions, and therefore in a position to explain these in court.

Should an investigator decide to tackle an email server and proceed down a forensic imaging route? This will probably cause the most inconvenience to the system users in terms of disruption, but will unquestionably provide the most complete

data, assuming a current timescale for the investigation, upon which to base the evidence.

What platform does the mail server operate on?

There is a significant difference between the skill set required to competently deal with a UNIX-based mail server, and a Windows-based mail server, or even (horror) a Mac-based system. No one has the skill set necessary to be competent in all hardware configurations and all software possibilities.

If someone is foolish enough to attempt to work on a large corporate system with which they have little or no experience or skill, the sound of the litigation team sharpening their swords will no doubt accompany the sound of the anguished cries from the system administrators as they almost inevitably kill the corporate mail system.

There is no shortage of advice to be found in forensic publications on how to deal with such situations, most of it bad, but ultimately there is no substitute for experience and practical knowledge.

The Anatomy of a Modern Mail Server

Assuming that an investigation team is technically competent to deal with a mail server, and to successfully image it, what are the next steps?

It is fair to assume that at this stage that an investigator would have a fair idea of what email system is being dealt with. Typically this would be a Microsoft Exchange Server, or Lotus Domino server with a technical complexity no greater than that, which could be reasonably anticipated.

It is worth looking at the similarities and differences between these systems to gain an appreciation of what has actually been captured during an investigation.

With an Exchange Server, the investigator is primarily interested in capturing the email server information stores, known as .edb files, the pub.edb and especially the priv.edb. The user's mailboxes can be thought of as a table of pointers that allows access to the data stored within the single .edb file. Generally there is a single priv.edb file (version 5.5 or lower), although it is possible in some instances that there may be multiple .edb files (2000 version or later).

A Domino server-based system by comparison has user mailboxes that are separate files, although a mailbox file may also be associated with multiple users. In most instances the Notes mail file will contain all of the data associated with that user, although there are situations where this is not the case, for example pointers to external object stores. Access to a database is by use of an .id file, which incorporates public/private key encryption technology.

Both systems have the option for email encryption to be set – 'simple', 'medium' and 'strong' under Lotus Domino Server, 'non', 'compressible' and 'strong' under Microsoft Exchange Server. Depending upon the circumstances of an investigation, this may add a certain technical complexity to the situation.

Both systems also have the facility to make local copies of emails to (typically) the user's computer. These local copies may be synchronised with the server information and may be considered dynamic, in that they contain links back to the server. Alternatively, they may simply be copies that do not synchronise with the server and can be considered as static copies. Under the Lotus Notes client these are known as duplicate or copy databases, under the Microsoft Outlook client they are known as .ost or .pst files. These will obviously be of interest to an investigation team, and a strategy to locate and digitally capture these in a sensible manner will be necessary.

There are other systems that operate in different ways and employ different technologies, and over time these systems will evolve. Understanding version 1.x of a system may not be sufficient to understand version 5.x of the same system.

Assuming that information can be captured in an evidentially acceptable and appropriate manner, and that further investigation of the email system is required.

Further technical issues

"If the only tool you have is a hammer, you tend to see every problem as a nail."

Abraham Maslow

The nature of the system and the scale and scope of the investigation will help define the most appropriate course of action. There is no single method that covers all eventualities and there are many tools on the market to do some of the work. These tools must be used cautiously and with some understanding of what may be achieved.

It is important that a scientific verification is possible for any result gained from a process. An essential prerequisite for any investigator should be a general understanding of the principles upon which any evidence is based. An investigator cannot be expected to have an exhaustive knowledge of everything, but should consider the questions that may be asked should they be challenged in court.

The issue of scale

Volume, content, and style of electronic communication has evolved from formal, precise business speak, to, frequently a convenient means of sending no more than the outline of ideas written in shorthand to an individual or group. What problem does this pose?

- **Scale**

It is currently fairly commonplace to forensically deal with servers in the many hundreds of megabytes or terabyte range. Today this seems quite large, next week or next year it will probably seem mundane or even quite small. The practical issue that this poses to a forensic investigation team is that they will initially need some comparability in their own storage systems to deal with this. They will then need to handle the volume of data in a meaningful way. This is a technical inconvenience, and one that can be easily overcome.

More significant however, is the sheer volume of information that this represents, and the need to deal with it during an investigation in a logical and accurate way. To put this into perspective it is not uncommon for a mail server to contain millions of emails. Some will be legitimate, sent internally, some will be from external sources, solicited and unsolicited. The issue of spam emails within an email system should not be underestimated. Email accounts set up for the purposes of spam research can receive in excess of 30,000 spam emails a day. Whilst this is obviously exceptional, it does illustrate the need for a powerful sorting mechanism.

- **Duplicates**

One of the benefits of a corporate email system is the ability to generate groups of people, and to then send emails to many at the click of a button, rather than have to type individual messages. Whilst in a business context this may be helpful, to the forensic investigator it can pose a significant problem. Hundreds of emails with identical content may seem helpful, but often it can simply obscure the key message.

- **Near Duplicate**

Possibly worse than duplicate emails, are 'near' duplicate emails. These again are usually generated initially by 'group' sending. Inevitably these invite replies, most contain no additional significant information other than to establish that they have been received. The reply is however a different email that needs to be tracked. The situation worsens because an individual email may generate a number of sub-threads, possibly involving different members or groups, each based upon the original common email, but splitting and evolving into a number of separate discussion threads. Following these threads effectively may require more specialist tools and techniques.

More Technical Issues to Consider

"For every problem there is a solution which is simple, clean and wrong."

Henry Louis Mencken

Unfortunately the very power that the modern email client affords the user can also increase the complexity that presents itself for the investigator to unravel.

Areas that can cause problems include (but not exhaustively):

- **Email Attachments**

These may be present and easily accessible, or may have been stripped from the email by the process of forwarding or by an option explicitly selected by the user. Worst deleted from the system. Recovery of deleted attachments is possible but, at best, it adds an extra level of inconvenience to the process and at worst the deleted email attachments may be missed. The issue of duplicates and near duplicates is also relevant to the matter of attachment.

- **Spam**

The issue of spam emails has already been discussed, however the broader issue of content should also be considered. An unfiltered mailbox may very well receive a large number of emails containing images of a pornographic (or worse) nature. The issue of intent should always be considered, especially where charges of inappropriate usage are raised. Simply being in receipt of an email, especially an unsolicited one, should not be considered as ground for further action, unless other evidence can be produced. This seemingly obvious statement is ignored all too frequently.

- **Viruses, Worms and Trojans**

Despite a tendency to use these terms interchangeably, they are quite separate and distinct entities. Use the terms with caution and precision, otherwise a technical report based on solid facts can have it credibility tarnished by obvious technical errors. From the investigation perspective the code that is most likely to be of interest will be Trojans, followed by viruses.

A Trojan is a piece of code that contains additional hidden functionality, most likely malicious in nature, which is unknown to the recipient of the code. The functions attributable to Trojan code are diverse, and can range from the merely irritating to the destructive. In the context of email, this is often a route into a system, let through by an incautious user and an unfiltered mail system. Depending upon the terms of reference of an investigation, the presence of a Trojan may have a great bearing on a case. The classic 'Trojan defence' is frequently incorrectly used as an attempt to muddy the evidential waters. This fact does not make the presence of Trojan code within an email system any less significant however.

A virus is a piece of code that infects another code, and usually carries a payload, again frequently malicious in nature, that is actioned when the virus carrying code is executed. Again the scope and nature of the payload can be highly variable. It should go unsaid that all systems should be protected by reputable and maintained anti-virus software, although this is not necessarily the case. Use of an anti-virus package does not guarantee that infection will not occur, and the nature of an infection and the precise timing must be considered carefully when looking at email (or any other) system.

Other sources of information

Whilst the email server is the primary source of information, an investigation team must not be blind to other sources of information that may support, or add to, the information that they already have access to.

Some examples of these are given below, although these are just simple examples and each investigation must considered on a case-by-case basis.

Email filter system – this may be configured to operate as a stand-alone system. The setting of the filters should be carefully examined, since they can impact upon the information that passes through to the user. If, for example, all executable files were automatically stripped from email attachments and quarantined, this may be significant supportive information for an investigation. Attachment size, extension, email content, are all items that can be used as filter criteria.

It may well be that the services of an application service provider (ASP) are used to pre-filter the emails reaching the mail company server. This may not be immediately apparent, and only an examination of, for example, the mail exchange (MX) records or perhaps the accounts system would reveal this fact. In this instance especially complex rules may be applied, some times many hundred that may well have a significant impact upon what is allowed in, and out of an email system.

Legal & Ethical Implications of an Investigation

Thus far the issue of the legislative framework within which a given investigation will be carried out has been avoided.

Obvious issues are the geographical locations of the data store, nature of the investigation, i.e. criminal or civil, whether the investigation is carried out for the owner of the data e.g. an internal disciplinary issue, or requires a search warrant or necessitates civil search and seizure order (or equivalent).

In the UK for example, a working knowledge of a diverse range of legislation may be required depending upon the nature of the case. This may include, the Police and Criminal Evidence Act 1984 (PACE), Electronic Communications Act 2000 (ECA),

Companies Act 1985 and Business Names Act 1985, Human Rights Act 1998, Data Protection Act 2002 (DPA), Computer Misuse Act 1990, Protection of Children Act 1978, and of course, the Regulation of Investigatory Powers Act 2000 (RIPA). The version 3 of the ACPO document: Good Practice Guide for Computer Based Electronic Evidence has recently been published. Whilst undoubtedly this has faults, and in many respects is a step backwards from version 2 of this document, it still contains some useful guidelines.

This list is by no means exhaustive, but does hopefully provide an indication of the breadth of legislation that the humble email can touch upon.

In any event, sound legal advice is a prerequisite before an investigation team embarks upon any potentially contentious course of action

The issues are frequently complex, and vary tremendously. In criminal cases the powers that a law enforcement agency can exercise are by no means uniform, and of course you may well be working for the defence rather than the prosecution.

There is of course an ethical aspect to an investigation of this nature. Defining legal boundaries is frequently difficult enough; however justifying an overtly intrusive investigative process, as being ethically defensible, can also be a matter of some spirited discussion.

Conclusion

The investigation of a complex modern email system is fraught with potential complexities: technical, legal and ethical. The skill set required to carry out all aspects of an investigation will not exist within a single individual. A blend of specific legal knowledge, up-to-date and highly specialist technical skills, coupled with investigative experience are required to bring an investigation to an appropriate conclusion.

Clive is Operations Director of Vogon International (www.vogon-international.com) He can be contacted on +44 (0) 1869 355255 or info@vogon-international.com

Security Waivers

Gordon Smith

Security officers are constantly identifying risks and taking steps to mitigate them in their quest to identify and eliminate security issues. One of the cornerstones of a protected network is strong policy, approved at the executive level and enforced by management. In many cases, legacy software or certain hardware technologies cannot conform to these policies. To facilitate the implementation of controls, whilst permitting some exceptions, management often implements a waiver system. Items that cannot meet the security or administrative policy are reviewed and granted an exemption, or waiver, for a period of time.

The waiver system is often abused, resulting in significant control issues. I strongly believe that the waiver system is used to provide legitimacy to flagrant policy violations that pose a significant threat to corporate security. Waivers increase the likelihood of fraud and malfeasance and perpetuate an unhealthy attitude towards control. Simply get a waiver if you can't comply with a control.

The waiver system is intended to enable management to grant temporary relief from a policy in specific instances when compliance is not possible. With the approved waiver in place, the vendors and staff have an opportunity to correct the issue and implement a safe and sane control solution. The waiver system also enables the early implementation of a policy that enhances controls. Even I believe that partial implementation is better than no implementation.

Waivers should not be granted every time there is an exception. Normally there is a committee that reviews the issues to determine if the problem truly cannot be fixed and that a waiver is justified. This committee may be composed of the CIO, senior IT management and senior members of the user community. This committee, in my mind, is not independent. They may want to sweep the policy violations under the carpet, defer problem resolution and, as a result, perpetuate control weaknesses. It is easier to approve a waiver than it is to fix the problem. I understand their position. Some legacy systems have inherent control weaknesses. It is expensive and labour intensive to replace this software with a new product.

Generally, waivers are granted for a three to six month period. Most of the waiver policies I reviewed permitted extensions, usually for a period not exceeding a year. Waivers cannot be renewed beyond the limitation period. I often find that waivers are frequently extended beyond the waiver limitation as no one is enforcing the waiver policy. I have never encountered an organisation that regularly audits waivers to ensure compliance and to identify items that fail to meet the required conditions for a waiver or items that exceed the time limitation.

Another concern that I have is that waivers may be granted even though compliance is possible. Sometimes funding issues causes this. In other cases, there may be a skills shortfall that prevents the organisation from properly implementing the required control. Most often, I find that management does not want to resolve the issue. These attitudinal waivers cause me great concern. Compliance is achievable, yet for whatever reason, the waiver is perceived to be the optimum solution in the minds of the business managers.

If your organisation chooses to use a waiver system, then there must be strong controls in place to ensure that waivers are only granted when justified, after a stringent and independent review process. The reason for the waiver must be clearly documented. The cost of remediation and the budget approval for the remediation effort should also be included with the waiver request. Any risks related to non-compliance should also be documented to ensure that management is aware of the business risk that they are accepting during the waiver period.

Waiver requests are often a result of operational issues. For example, I often see waivers on database exports or backups. When an application is implemented, there is usually no

problem performing the required exports and backups. As time passes, the databases grow and nightly batch processing may expand to the point where the backups cannot be completed before the start of the next business day. Rather than addressing the performance issue, a waiver is granted that permits an incremental export or backup. Over time, database growth causes the timeframe for incremental export to exceed the time available. When this occurs, a waiver is granted so that the incremental export or backup is performed twice a week or on weekends.

The real solution would be to find the cause of the performance degradation. This is normally insufficient physical memory causing unnecessary overhead, under powered hardware, poorly structured database indices or inefficient SQL or SQR programs. Finding and fixing these issues requires a very good DBA and performance tuning tools or utilities. It is easier to get the waiver than fix the problem. Easier that is, until disaster strikes! Days or even weeks worth of data could be lost if the database cannot be properly recovered.

I also find waivers used when passwords cannot be changed. Some of the common excuses I hear are that the vendor or contractor require a standard password so that they can perform emergency maintenance. If a standard password is used, you can be sure that hackers will learn of this quickly, enabling the hacker to easily compromise your system. I have also seen password waivers used for database access accounts. PeopleSoft and other such applications use these accounts to access the Oracle database. These passwords are often created during application development when there are many contractors who "must have the password" to build and test their modifications. When the application goes into production, the password is not changed. Furthermore, because of the "large number of SQL and SQR programs with embedded passwords," the password cannot be changed. A waiver is granted, and the application is highly exposed to unauthorised access and update by the large number of people who know the password. If the SQL and SQR passwords are poorly secured, then the application is also highly exposed should a hacker or disgruntled employee gain access to the password that is stored within these programs in clear text.

Sometimes organizations grant modem waivers to enable the administrators to bypass the VPN or firewall to perform emergency maintenance should the firewall or ISP fail. These modems do not have secondary authentication in place. When we suggest that the modem be restricted or controlled using secondary authentication or biometrics, we are told that there is a waiver in place and the client is permitted to keep the modem. This is foolhardy to say the least.

We occasionally find waivers granted so that machines do not have to be patched. This is normally due to vendor software products that will not work if patches are installed. Rather than force the vendor to correct the issue, the waiver grants them an exception. As a result, the machine is exposed to a security or performance issue that can seriously interrupt processing or permit the system to be compromised by hackers, contractors or disgruntled employees.

Many of the above items can cause serious issues with the Sarbanes-Oxley Act of 2002, a public company accounting reform and investor protection act. Within this act there are specific requirements for disclosing information technology risks. Some of the risks, for which waivers have been granted, will need to be disclosed or the organisation may face penalties or even criminal charges for non-disclosure. All waivers need to be reviewed on a regular basis to determine if there are Sarbanes-Oxley issues. Wise auditors and security officers will use the disclosure requirements to discourage the renewal of existing waivers and prevent the issuance of new waivers that cause Sarbanes-Oxley disclosures.

Waiver tracking is also very important. Often management does not know the cumulative risk of outstanding waivers. A summary of each waiver and the specific risks should be provided to management. I believe that management will quake in their boots when they understand the cumulative risk of outstanding waiver issues.

Another good practice is to perform a periodic impact analysis of the highest risk items. Management needs to know the business impact should the risk underlying the waivers occur. Keep in mind that the waiver system documents known risks and management's acceptance of those risks. As a result, the waiver system and specific waivers could be used against the organisation should there be civil litigation. Damages could be increased if the organisation is deemed to be negligent. Legal negligence may occur if management had prior knowledge of an issue, that the occurrence of the issue has a significant cost, and that management chose to accept the risk when a prudent person would not accept that same risk. Imagine how foolish a company would look in court if a plaintiff was able to prove that management had a policy to patch machines and that a waiver was obtained to enable non-compliance to the policy. A company machine is then infected with a worm or virus and attacks other companies, creating a costly Information Armageddon. Victims of the forwarded virus or worm could sue the company in a heartbeat and likely win. In addition to the costs of defending the case, the damages, and penalties, this would be a significant public relations nightmare.

Management should also be notified on a quarterly basis of all permanent waivers and any waivers which have been renewed two or more times. Extensions, while intended to provide a little more time to achieve compliance, are often abused. Ensure that management receives periodic reporting of the expiry dates of critical waivers. This enables management to encourage staff to remedy the issue, eliminating the need for further waivers.

The waiver review process is much easier if there is a waiver database. This should document the reason for the waiver, the expiry date, the risk level, and business impact if a control breakdown occurs. The budget for the remediation and the percentage of completion should also be tracked in this database. Lastly, management should ensure that the appropriate staff is assigned for the task of remediation and that it occurs on a timely basis. If your existing staff cannot implement the required remediation, then hire someone who can.

As you can see, I feel very strongly about waivers. I believe that they are occasionally required, provided there is a concerted effort to bring the issue into compliance. Also, management must actively support the remediation efforts. Waivers that extend beyond a year can greatly increase business risk and expose the organization to excessive costs or a public relations disaster should a control violation occur. I strongly suggest that a full waiver system audit be performed annually as part of the general controls review.

Gordon Smith is President and CEO of Canaudit, Inc. He can be contacted at gordon@canaudit.com.

The Down Under Column

Bob Ashton – IRMA Oceana Correspondent

QUO CUSTODIET IPSOS CUSTODES?

A recent press report stated that a claim of Certified Information Systems Auditor (CISA) accreditation of a senior staffer of a State Government Audit Office made in that organisation's annual report was false. Elizabeth de Wolf of the Information Systems Audit and Control Association (ISACA) confirmed that the staffer's right to use the CISA designation had expired in December 2001. The report went on to question the quality and validity of audits performed under the supervision of a person falsely claiming a professional qualification.

British Standard 7799 Clause 6.1.2 recommends that confirmation of claimed academic and professional qualification be carried out at the time of job application.

In order to safeguard against the reputational risk highlighted by this case, best practice may require that claims of professional qualifications need to be validated on an annual basis, rather than once only. This is particularly so in the case of information and communication technology qualifications, including CISA, which require proof of continuing professional education by practioners. This would be an easy task for any employer to undertake as it would require no more than an email to the sponsoring body requesting a statement of the accreditation status of employees, yet such a low cost risk mitigation strategy appears to be the exception rather than the rule.

ISACA, the sponsoring body of CISA has been most responsible in protecting the interests of employers of ICT auditors and users of ICT audit services by its strong policies in regard to continuing professional education, as it is clear to most working in this field that ICT audit knowledge can quickly become obsolete. Unless practitioners make serious efforts to maintain the currency of their knowledge, at best it will quickly become irrelevant, and at worst may provide a false sense of comfort to clients as critical emerging issues will be ignored. A good example of the latter are the risks presented by wireless LANS. An auditor with inadequate and out of date knowledge and skills may concentrate his attention on the controls within a financial application, while ignoring the fact that passwords providing access to that application were being broadcast far and wide by an inadequately secured wireless LAN.

ISACA's procedures in the area of continuing professional education are reflected in the following ICT security related qualifications:

- Certified Informations Systems Security Professional (CISSP) sponsored by the Information Systems Security Association (ISSA) which requires annual continuing education to maintain certification.
- The Global Information Assurance Certificate program, founded by the Systems Administration and Network (SANS) Institute, which requires that certifications are renewed every 2 years by taking, and passing, a "refresher" exam, and
- Microsoft Certified Engineer (MSCE) Security Specialization, which requires that additional exams are passed when new software platforms are released.

The AON European Risk Management & Insurance Survey 2003 identified that the risk of loss of reputation was considered to be second only to that of business interruption. In order to avoid unnecessary reputational risk, and to avoid the management ineptitude displayed in the case described, a responsible management may wish to follow the simple procedure recommended, and avoid the professional opprobrium resulting from false professional accreditation claims.

From the Cash Box

Jean Morgan – IRMA Treasurer

The group's finances are improving again. Our first chargeable event of the year, November's "E-mail Management and Security" was a joint event with the IT Faculty of the ICAEW. This resulted in a surplus for each party of £1711.35 after all expenses. Our second chargeable event of the year on Network Management will have taken place by the time you read this. These events normally form the biggest source of our funds each year, with subscriptions second.

On a non-Treasurer subject, I have just received an email which might interest some members. In the past I have tutored a couple of Open University residential schools (in Creative Management, if you must ask). The OU is now trying to recruit tutors for a brand new course, 'Information security management'. This is scheduled to start in November 2004 but will pilot sooner and seems to be a Masters level course. If you're interested in knowing more, please email me (jean@wilhen.co.uk) and I will forward the email details.

BCS MATTERS!

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

Information is also available from Customer Services at The British Computer Society, 1 Sanford Street, Swindon, SN11HJ (e-mail to marketing@hq.bcs.org.uk)

The New BCS Grading Structure

The BCS is moving ever closer to the implementation of the new grading structure outlined in the last edition of this Journal. At that time, late 2003, we had completed the first, critical stage of the process, which involved gaining the support of the existing Members and Fellows at an Extraordinary General Meeting (EGM). Because the new structure involves a change in the royal charter and by-laws, we needed a 75% vote in favour at the EGM; in the event, the yes vote was in excess of 97% - a very emphatic endorsement of the proposals.

The next stage in the process involved a submission to the Privy Council for approval to the necessary changes to the Charter and By-laws. That stage has also been completed successfully and we now have a team within BCS HQ working to implement the new structure on 1 May this year.

The key feature of the new arrangements is the separation of the existing Chartered professional membership (MBCS and FBCS) into two elements – professional membership and chartered status. Each element will have its own application process and its own designatory letters; professional membership will retain the existing letters *MBCS* and *FBCS* whilst chartered status will now be designated by the addition of the letters *CITP* and the title *Chartered IT Professional*.

The aim of all this change is to make BCS membership – especially professional membership – more accessible to a larger cross-section of qualified competent IT practitioners. By separating chartered status from professional membership, the new arrangements will allow us to offer the Member grade, with the right to use the post-nominal letters MBCS, at a much earlier career point. Gone will be the requirement for up to 10 years experience; applicants for MBCS will now need a maximum of 5 years ICT experience even if they hold no recognised academic qualification. With relevant qualifications, this experience requirement reduces and those with the highest level of BCS professional examinations or a degree at honours level accredited by the BCS will be eligible for MBCS at the point of graduation.

Rapid Application Processing

Speed of completion of the application process is an essential element of the new arrangements. From 1 May, potential members will be able to apply by completing a very simple on-line form and our aim will be to admit eligible applicants to professional membership within three days of the application. That will require the complete streamlining of all aspects of the application process and the maximum use of what will be known as *'Trusted Sources'* – organisations and individuals on whose validation and recommendation we can rely absolutely when admitting new professional members. Such sources will include a range of organisations, from IT employers to other professional bodies, specifically licensed by the BCS. The interest being shown by the employer community is particularly encouraging and we are currently in discussions with a number of large employers on the basis of arrangements which range from simple endorsement of applications to schemes under which large numbers of staff will be admitted en-bloc.

BCS Branches, Specialist Groups and our existing Chartered Professional members will also be important trusted sources. In essence, we believe that if a Branch, Group or a chartered professional member is prepared to vouch for the professionalism of a colleague – within a few simple parameters – then that recommendation should be accepted without the need for further processing. Within the course of the next few weeks, well before the start date of 1 May, the President, Wendy Hall, will be writing to all Members and Fellows, Branches and Groups, encouraging them to nominate eligible colleagues to be invited to join the BCS as professional members.

BCS Chartered status

Following the separation mentioned above, Chartered status will be available exclusively to BCS professional members, as an add-on to their membership. The existing rigorous assessment procedures, including the requirement for interview in some cases.

Although processing for chartered status will inevitably take longer than that for professional membership, we will also be looking for ways of significant streamlining, and for extending the trusted Source concept, to the chartered status process. In this context, we have recently agreed with one organisation – IBM – that the processes it uses for higher levels of its professional structure are sufficiently rigorous to be fully accredited by the BCS for admission directly to chartered professional membership. This will mean that applicants at the level of IBM Certified professional will be accepted into BCS chartered professional membership without the need for further processing. In essence this arrangement shifts the processing burden from the quality control of individual applicants to the quality assurance of the source organisation. It provides very real gains for everyone involved – BCS, employer and applicant – and we will looking to extend the arrangement to other employers that have the necessary professional structures and processes in place.

Engineering Council and Other Qualifications

Engineering Council qualifications, *Incorporated* and *Chartered Engineer*, will continue to be available to BCS Chartered professional members on the same basis as at present. Eligibility for such qualifications will generally be picked up at the point at which a member applies for BCS chartered status and will be taken forward as part of a combined process.

We are currently looking at other Chartered qualifications which might be appropriate to BCS members, including the new Chartered Scientist qualification for which we have submitted an application for licensed status.

New Services for members

Reducing processing bureaucracy will be a major advance for the Society and we are confident that it will attract very many new members. Retaining those new members will, of course, require more than a reduction in bureaucracy and we recognise the need also to improve the services that we offer to members. There are a number of new services in the pipeline including a new on-line *Individual Career Manager* service which will provide members with career planning tools built around the BCS *Industry Structure Model (ISM)*. This service is scheduled for release before 1st May and will be the first of a number of new products and services built around the ISM, including a *Professional Experience Record* service aimed principally at the independent contractor community.

New ISEB Qualifications

Also in the pipeline is a substantial expansion of the very successful IS Examinations Board portfolio of vocational qualifications. Most are under development within Malcolm Sillars Product Development Unit but one, the Foundation Certificate in Project Management, was released in early February.

The certificate is suitable for anyone involved in IT projects or new to project management wishing to achieve a grounding in the fundamentals of the subject. It will provide visible evidence that candidates understand the principles of project management including project planning; monitoring and control; change control and configuration management; effort estimation; quality and risk management and communication between stakeholders.

There are no prerequisites for taking the certificate, although a basic working knowledge of IT is essential and it is recommended that candidates attend a suitable ISEB training course with one of the accredited training providers to prepare for the one hour multi-choice examination.

Further expansion to the ECDL portfolio

The range of new qualifications within the European Computer Driving Licence portfolio also continues to grow – most recently with the launch of a new BCS *Equal*Skills programme designed to provide a first step on the ladder to computer literacy.

Nearly a third of the UK's population are being left behind in our increasingly information driven society, thwarted by a genuine fear of attempting to use a computer. The new BCS programme is intended specifically for such technophobes and promises to enable a major part of society with the rudiments of IT communication skills.

The new *Equal*Skills course will shortly be available from adult education institutes and local training providers. It is a short, staged training and assessment programme with a certificate awarded on successful completion to acknowledge achievement. The programme will be fun, informal and easy-to-use and will show newcomers to IT the very basics of computing from learning how to switch on a computer, use a mouse to exploring the internet for the latest weather updates and holiday bargains.

And Finally……

As part of a major expansion of its publishing programme, the BCS has launched a subscription service designed to keep you informed about new BCS products and services. There are currently 10 new publications in production – focused mainly on the issues at the interface between IT and the business - and, if you sign up to the new service, details will be emailed direct to your inbox. To subscribe, just send a blank email to:- publications@lists.bcs.org.uk

HUMOUR PAGES

Ever Wonder . . .

...why the sun lightens our hair, but darkens our skin?

...why women can't put on mascara with their mouth closed?

...why you don't ever see the headline "Psychic Wins Lottery"?

...why "abbreviated" is such a long word?

...why doctors call what they do "practise"?

...why you have to click on "Start" to stop Windows 98?

...why lemon juice is made with artificial flavour, while dishwashing liquid is made with real lemons?

...why the man who invests all your money is called a broker?

...why there isn't mouse-flavored cat food?

...who tastes dog food when it has a "new & improved" flavour?

...why Noah didn't swat those two mosquitoes?

...why they sterilize the needle for lethal injections?

...why they don't make the whole plane out of the material used for the indestructible black box ?

...why sheep don't shrink when it rains?

...why they are called apartments when they are all stuck together?

...if con is the opposite of pro, is Congress the opposite of progress?

...why they call the airport "the terminal" if flying is so safe?

Instruction Labels

In case you need further proof that the human race is doomed because of stupidity, here are some actual label instructions on consumer goods.

On a Sears hairdryer: Do not use while sleeping. (and that's the only time I have to work on my hair).

On a bag of Fritos: ...You could be a winner! No purchase necessary. details inside. (the shoplifter special)?

On a bar of Dial soap: "Directions: Use like regular soap." (and that would be how???....)

On some Swanson frozen dinners: "Serving suggestion: Defrost." (but, it's "just" a suggestion).

On Tesco's Tiramisu dessert (printed on bottom): "Do not turn upside down."(well...duh, a bit late, huh)!

On Marks & Spencer Bread Pudding:"Product will be hot after heating." (...and you thought????...)

On packaging for a Rowenta iron: "Do not iron clothes on body." (but wouldn't this save me more time?)

On Boot's Children Cough Medicine: "Do not drive a car or operate machinery after taking this medication." (We could do a lot to reduce the rate of construction accidents if we could just get those 5-year-olds with head-colds off those forklifts.)

On Nytol Sleep Aid: "Warning: May cause drowsiness." (and...I'm taking this because???....)

On most brands of Christmas lights: "For indoor or outdoor use only." (as opposed to...what?)

On a Japanese food processor: "Not to be used for the other use." (now, somebody out there, help me on this. I'm a bit curious.)

On Sunsbury's peanuts: "Warning: contains nuts." (talk about a news flash)

On an American Airlines packet of nuts: "Instructions: Open packet, eat nuts." (Step 3: maybe, uh...fly Delta?)

On a child's superman costume: "Wearing of this garment does not enable you to fly." I don't blame the company. I blame the parents for this one.

On a Swedish chainsaw:"Do not attempt to stop chain with your hands or genitals." (...was there a lot of this happening somewhere?)

Just in Case you Think Syntax isn't Important . . .

Take a look at what happens when your tongue gets wrapped around your eyetooth and you can't see what you're saying. These are newspaper headlines that actually appeared in print:

* Iraqi Head Seeks Arms
* Stud Tires Out
* Prostitutes Appeal to Pope
* Panda Mating Fails; Veterinarian Takes Over
* British Left Waffles on Falkland Islands
* Eye Drops Off Shelf
* Teacher Strikes Idle Kids
* Juvenile Court to Try Shooting Defendant
* Two Sisters Reunited After 18 Years in Checkout Counter
* Killer Sentenced to Die for Second Time in 10 Years
* Never Withhold Herpes Infection From Loved One
* If Strike Isn't Settled Quickly, It May Last a While
* Cold Wave Linked to Temperatures
* Red Tape Holds Up New Bridge
* Typhoon Rips Through Cemetery; Hundreds Dead
* New Study of Obesity Looks for Larger Test Group
* New Vaccine May Contain Rabies
* Prosecutor Releases Probe Into Undersheriff

Actual quotes from employee performance reviews

I would not allow this employee to breed.

This associate is really not so much as a has-been, but more of a definitely won't-be.

Works well under constant supervision and cornered like a rat in a trap.

When she opens her mouth it seems it is only to change whichever foot was previously there.

He would be out of his depth in a parking lot puddle.

This young lady has delusions of adequacy.

He sets low personal standards and then consistently fails to achieve them.

This employee is depriving a village somewhere of an idiot.

This employee should go far and the sooner he starts, the better.

Not the sharpest knife in the drawer.

Got into the gene pool when the lifeguard wasn't watching.

A room temperature IQ.

Got a full 6-pack, but lacks the plastic thingy to hold it together.

A gross ignoramus – 144 times worse than an ordinary ignoramus.

A photographic memory but with the lens cover glued on.

A primary candidate for natural deselection.

Bright as Alaska in December.

One-celled organisms outscore him in IQ tests.

Donated his brain to science before he was done using it.

Fell out of the family tree.

Gates are down, lights are flashing, but the train isn't coming.

Has two brains: one is lost and the other is out looking for it.

He's so dense light bends around him.

If brains were taxed she'd get a refund.

If he were any more stupid he'd have to be watered twice a week.

If you give him a penny for his thoughts you'll get change.

If you stand close enough to him you can hear the ocean.

It's hard to believe he beat 1,000,000 other sperm.

One neuron short of a synapse.

Some drink from the fountain of knowledge, he only gargled.

Takes him an hour and a half to watch 60 Minutes.

Wheel is turning but the hamster is dead.

Since my last report this employee has reached rock bottom and has started to dig.

His employees would follow him anywhere, but only out of morbid curiosity.

And finally . . .

"Genius may have its limitations, but stupidity is not thus handicapped."
Elbert Hubbard (1856-1915), American author.

Member Benefits

Mark Smith

IRMA is pleased to announce that we have negotiated members' discounts on the purchase of a number of software packages:

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)**

We are looking to extend this range of discounts to include additional 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 our Members' Benefits Officer (Mark Smith, **mark.smith@lhp.nhs.uk**) who will be happy to approach suppliers.

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

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

CHAIRMAN	John Bevan	john_bevan@ntlworld.com
DEPUTY CHAIRMAN	Alex Brewer	alex.brewer@morganstanley.com
SECRETARY	Siobhan Tracey	siobhan.tracey@booker.co.uk
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Celeste Rush	rushlse97@aol.com
JOURNAL EDITOR & SECURITY PANEL LIAISON	John Mitchell	john@lhscontrol.com
WEBMASTER	Allan Boardman	allan@internetworking4u.co.uk
EVENTS PROGRAMME MANAGER	Graham Devine	graham@grahamdevine.me.uk
EVENTS PROGRAMME CONSULTANT	Raghu Iyer	raguriyer@aol.com
LIAISON - IIA & NHS	Mark Smith	mark.smith@lhp.nhs.uk
LIAISON - LOCAL AUTHORITY	Peter Murray	cass@peterm.demon.co.uk
LIAISON - ISACA	Ross Palmer	ross.palmer@hrplc.co.uk
MARKETING	Wally Robertson	williamr@bdq.com
ACADEMIC RELATIONS	David Chadwick	d.r.chadwick@greenwich.ac.uk
	David Lilburn Watson	dlwatson@bcrm.co.uk

SUPPORT SERVICES

ADMINISTRATION	Janet Cardell-Williams t: 01707 852384 f: 01707 646275	admin@bcs-irma.org
LIAISON - KPMG	David Aurbrey-Jones	david.aubrey-jones@kpmg.co.uk
OR VISIT OUR WEBSITE AT	**www.bcs-irma.org**	Members' area Userid = irmamembers Password = irma2004

BCS IRMA SPECIALIST GROUP ADVERTISING RATES

Reach the top professionals in the field of EDP Audit, Control and Security 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 (Monochrome Only) 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

Inserts can be included with the Journal for varying advertising purposes, for example: job vacancies, new products, software.

Insertion Rates:

For inserts weighing less than 60grams a flat fee of £300 will be charged. Weight in excess of this will incur additional charges:

- 60-100grams: 14p per insert
- 101-150g: 25p per insert
- 151-300g: 60p per insert
- 301-400g 85p per insert
- 401-500 105p per insert

Thus for an insert weighing 250g it would cost the standard £300 plus weight supplement of £210 (350 x 60pence) totalling £510.

Discounts:

Orders for Insert distribution in four or more consecutive editions of the Journal, if accompanied by advance payment, will attract a 25% discount on quoted prices.

Direct mailing

We can undertake direct 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 plus a handling charge.
Access Charge £350. Please note photocopies will be charged at 21p per A4 side.

Personalised letters:

We can provide a service to personalise letters sent to our members on your behalf. This service can only be provided for standard A4 letters, (i.e. we cannot personalise calendars, pens etc.). The headed stationery that you wish us to use must be received at the Office at least ten working days before the distribution is required. Please confirm quantities with our advertising manager before dispatch. If you require this service please add £315 to the Direct mailing rates quoted above.

Discounts: Orders for six or more direct mailings will attract a discount of 25% on the quoted rates if accompanied by advance payment

Contacts

Administration

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

BCS IRMA Specialist Group Advertising Manager

Eva Nash Tel: 01707 852384
Email: admin@bcs-irma.org

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

BCS
THE BRITISH COMPUTER SOCIETY

Membership Application

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

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

CORPORATE MEMBERSHIP (Up to 5 members)* *Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal *(see over)*	£75
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). Educational Establishment: _____	£10

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

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

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

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

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY:

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

Venue for

Full Day Briefings

Old Sessions House
Clerkenwell Green
London EC1

Venue for

Late Afternoon Meetings

KPMG
8 Salisbury Square
London EC4