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

JOURNAL
volume 14 number 3 summer 2004 ISSN 1741-4229

Programme for members' meetings 2004 – 2005

Tuesday 7 September 2004 Late afternoon	**Computer Audit Basics 2: Auditing the Infrastructure and Operations**	16:00 for 16:30 KPMG
Thursday 7 October 2004 Full day	**Regulatory issues affecting IT in the Financial Industry**	10:00 to 16:00 Old Sessions House
Tuesday 23 November 2004 Full day	**Internet Security and Networks**	10:00 to 16:00 Chartered Accountants Hall
Tuesday 18 January 2005 Late afternoon	**Database Security**	16:00 for 16:30 Central London
Tuesday 15 March 2005 Full day	**IT Governance**	10:00 to 16:00 Old Sessions House
Tuesday 17 May 2005 Late afternoon AGM precedes the meeting	**Computer Audit Basics 3: CAATS** ***Preceded by IRMA AGM***	16:00 for 16:30 Central London

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 May	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

I get back from one of my trips abroad, plug my laptop into my LAN and find that I cannot access the Internet or my email. Everything was working okay before I went away and everything worked fine in the hotel abroad which had a wireless LAN, but back at the ranch it is a complete no-no. So I start fiddling with my settings; shutting down programs that have loaded at start-up without any problems for years, deactivating my firewall and all the other things that one does when slightly jet lagged and perhaps not thinking too clearly. My dial-up link continues to function as normal so I use that, in between sessions of trying to solve my broadband problem, to update my anti-virus software and access my email. After a few days my broadband email starts working, albeit on an very intermittent basis. As I know that my email uses my Internet settings I expect my Internet access to be restored on the same intermittent basis, but it will have none of it. I check with my neighbour, who uses the same broadband provider and local telephone exchange and his service is fine. But then he uses a Mac, so I start suspecting that this must be a Windows XP problem associated with the Sasser worm, even though I check for anti-virus updates every four hours and Windows updates daily (I know that this may seem over the top, but in my job you can't afford to let your guard down). To be on the safe side I re-check for critical updates (zilch), anti-virus updates (zilch) and do a complete virus scan (zilch).

So I contact the BT Yahoo support desk and after the usual wait go through the problem with a support person. I mention the intermittent email, the error message I receive when attempting to access the Internet, the fact that my dial-up works fine and that I am sitting behind a broadband router. He asks about the router and I give him all the details. He suggests renumbering the IP address that the router uses to access the BT Yahoo DNS server. I make the change he suggests to the IP address, but to no avail. I then plug into my USB port the old broadband modem that came with the original BT package and after downloading the updated driver (the original crashed the computer) everything works okay. As this modem gets the DNS IP address automatically I become convinced that either my router got fried in a thunderstorm that occurred whilst I was away or the DNS address is wrong. Either of these theories is supported by the fact that I can't get any of the other computers on the LAN to access the Internet either. I re-contact the support desk and ask whether they have changed the IP address of their DNS? Their response is that they haven't, so I try each IP address they give me in turn, but to no avail. I check the help page on their web site and the DNS addresses stated there agree with the ones provided by the support desk.

Totally frustrated I use my search engine for clues and find out that while I have been away BT Yahoo had changed their entire broadband infrastructure for security reasons, including the IP addresses of their Domain Name Servers, but they haven't bothered to tell their customers! The web is alive with complaints. I should have searched it earlier Grrrrr! As none of the complainants provide the new DNS addresses, I email the BT support desk (I couldn't face the friendly, but useless staff at the other end of the 'phone) and receive an automatic response directing me to the FAQ part of their web site. I check this only find the old DNS addresses. The auto response does however, allow me to fill in a form describing my problem which I do, but pointing out that all I need is the new DNS addresses. I receive an auto reply which is the exact same message as the first time around! Totally frustrated I write how crazy this is and send it off only to receive the self-same auto response. Grrr again. So I use a bit of nowse and by using the old BT broadband modem and the ipconfig command I am able to see the DNS address that it is picking up. I program this into my router and lo and behold the Internet springs to life. The next day I receive an apologetic email from the support desk giving the address that I had already found.

I had now spent two weeks trying to solve the problem and the solution was a simple two minute change to the DNS address in my router! The arrogance (or incompetence) of BT Yahoo is staggering. To make a major infrastructure change without giving its customers a key piece of information is incompetence of a large order. The web complaints were indicating that 300,000 customers had been affected. If this figure is true and if each one of those customers was off the web for two weeks as I was, then the country incurred a total productivity loss of over 11,500 man years, plus the equivalent waste in management time in trying to solve the problem. A staggering total of around 23,000

wasted man years to UK plc. The fact that neither the support desk or the FAQs were aware of the problem and continued to give me wrong information over that period indicates a lack of decent change management. I complained to the BT Chairman, Sir Christopher Bland and received an initial holding response followed up by a telephone call from someone at the BT Open World 'High Level Complaints' Team. I queried whether BT Yahoo was accredited to ISO 9000, but he didn't know. He couldn't answer my other questions either, but has said that he will get back to me. I will update you in the next edition.

To my own chagrin, my subsequent root cause analysis, which is something I do after every problem, showed that all the clues for an early diagnosis and solution were staring me in my face. First, I hadn't made any significant changes to my configuration while abroad as the hotel had an internal LAN with broadband connectivity through a router. The sole change had been to my email account to use my Net2Roam server because the ISP used by the hotel didn't allow relaying from my BT Yahoo account, but I had changed this back before connecting into my own LAN. The fact that none of my other computers could access the web (and none of their settings had altered) indicated either a router or a BT Yahoo problem. I was initially mislead by the potential lightning strike, but I should have discounted that as soon as I started to get an intermittent email connection which pointed to a service infrastructure problem, rather than something at my end. The main clue however, was the Internet error message 'dnsserver error', but as the support desk said that there were no problems with their DNS and also that the DNS address in my router was correct, I was mislead into thinking that the problem was elsewhere. Next time I will check the web first to establish if other people have a similar problem and this brings me to my final point of this sorry saga. Why doesn't BT Yahoo check the web themselves on a regular basis, as an early warning indicator, that things are going off track? As an auditor I always check the complaints 'book' to ascertain whether the customers have any problems with the service being provided.

On to better things. Two follow-up articles in this edition. One from Greg Krehel dealing with creating a 'cast of characters' to help with your investigations and another from Priscilla Emery dealing with the importance of document management in business continuity planning. Both of these articles are continuations of themes in the last edition and will be continued into the next. We also have a great article on PDA security from Didi Barnes of First Base. Our new Chairman, Alex Brewer, re-establishes the message from the Chairman column and Colin Thompson from the BCS updates us on what is happening elsewhere in the Society. I have already used the new membership grades that Colin described in the last edition to nominate two IRMA Committee members for professional membership (you see there is some benefit from being a committee member). Celeste Rush, our Membership Secretary, provides an analysis of our membership which may be of interest to those of you of a demographic analysis bent.

Summer is here and the holiday period is almost upon us. Not for me however, as there is the Autumn edition to consider. Happy reading.

John Mitchell

Membership

The new 2004/5 season will mark the 40th anniversary of the IRMA specialist group. Over the course of the years it has been called different names (no puns) but still remains the longest BCS security specialist group in existence. In the next Journal I hope to be able to give some of the history of IRMA from its inception to the present for your information. In the meantime the new season looks like it will be both interesting and informative.

On the subject of the membership, I recently had a chance to view IRMA's membership statistics for 2003/4 and thought I would take this opportunity to share this information with you here.

The total membership for 2003/04 was 236. Of these, 73 members were from the London region, 160 from the rest of the UK, and 3 from overseas.

IRMA has six different Membership Categories:

Corporate	22
Corporate Sub	61
Individual BCS	61
Individual non-BCS	69
Courtesy (e.g. speakers)	19
Student	4

There are also six Professional Categories:

Internal audit	138
External audit	18
Data Processor	10
Academic	2
Student	6
Other	62

As one might expect the Internal Auditors take the prize!

As always, the committee is keen to offer value for your membership and would appreciate your comments and views, especially any requests for a particular topic you would like the monthly meetings to cover, be it full day or evening.

I look forward to seeing you in September.

Celeste Rush

From the Chairman

'May you live in changing times'

As incoming chairman, I would like to thank John Bevan for chairing the IRMA group for many years. He is still on the committee, and for his day job is now working at BCS HQ with all of the specialist groups, and so is well placed for the odd query from the IRMA committee! I would also like to thank all of the current committee for their hard work during the year.

During March this year, the committee appointed me to the chairman for the group and so far, it has been an eventful time for all of us.

We are all watching the world price of oil rise as demand outstrips supply. Companies continue to offshore and outsource key parts of their infrastructure. Some companies have changed their minds and brought some activities back in house.

In the last quarter in my work role I see the continuing exponential rise of spam, including fraud (or 'phishing' attacks). The Sasser and Netsky worms threaten the integrity of our systems.

To interpret these events and their impact on our organizations requires the input of informed and alert risk management professionals, and it seems to me that the more uncertain the environment becomes, the more our skills are in demand.

IRMA's role

To that end IRMA continues to supply two key items:

- Training
- A network of people.

I think the second item is often overlooked. If you have pressing issues, why not bring them to the next meeting and discuss them with the attendees, starting with the famous words 'I have a friend'? Please make use of the people network.

As well as the people network, we also wish to gather but not misuse your email addresses and create a 'virtual' network. The aim here is to promote discussion and to speed up communication between the committee and the members. Also on the horizon, the BCS wishes to wake the 'sleeping giant' of its Specialist Group membership, and to ask for comment about forthcoming white papers and other government and industry initiatives. An example of one of these discussions that took place recently was identity cards, which was also in the news.

This means that IRMA's role as an people network is broadening out to a network of members also connected to the BCS and on into public life.

Watch this space or your inbox for further details. If you have not provided us with your email address yet, please email admin@bcs-irma.org, and don't forget to mention your IRMA number.

BCS membership changes

The BCS wishes to assume a greater profile to government, within the IT industry, and academia. As part of this there is now a significant drive to recruit professional members. Their recruitment process for membership was famously difficult and off-putting, and to correct this they have changed their charter to allow professional members of the society, vetted by existing chartered members and trusted sources, of which this group is one.

As well as this, normal IRMA members can also become associate members of the BCS for a nominal fee, which reduces your IRMA subs from £25 to £15.

Our normal activities for 2003/4

During the year, IRMA ran the following events:

- Wireless Networking Update
- Email Management and Security
- PDAs and mobile computing risk
- Audit planning
- Network management and security
- Server farms

Unfortunately, we cancelled 'Security in Outsourcing' because of apparent lack of demand, which surprised the committee, because of the sheer scale of outsourcing at the moment. Next year's programme has been drafted.

Other AGM highlights

If you would like a copy of the accounts please contact admin@bcs-irma.org. During the year we made a deficit of approximately £4,300, however our reserves are healthy so this is not an issue for now.

Much more of concern is the deficit of people committing time to help run the specialist group, and the number of members, which has continued to fall. For the retention of members, I believe that if we perform our normal training activities well, and improve links with our members, that the group can once again flourish.

And finally...

It now falls to all of us to widen our network and committee with significantly more support from the BCS than we have previously had - I hope you are able to join us on our journey. Please contact the committee with any ideas you have (admin@bcs-irma.org).

Alex Brewer

Case Investigation - The Cast of Characters

Greg Krehel

This is the second in 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 identifying the principle and supporting characters in a case – Ed

Do you create a Cast of Characters for every case? What could be easier and more basic? Despite its simplicity, a cataloging of key players is of great value. It can be an important aid during early witness interviews, as you evaluate case risk and compare your analysis to others on the trial team, as you brainstorm on the order in which to present evidence at trial, and when you need to bring new trial team members up to speed on a case. The following article presents some ideas on how to create a great Cast of Characters. I think you'll find these ideas easy to apply. And I hope you'll find them effective. If I'm successful, you'll see new possibilities for an old tool.

Think Outside the Witness Box

To make the most of your Cast of Characters, you should treat it as far more than a witness list. It should serve as a catalogue of all critical things in the case: persons, organizations, documents, other physical evidence … any important thing. Taking this broad approach makes your Cast of Characters far more valuable when you want to use it to reflect, evaluate, and educate. You've no doubt heard the expression "Think outside the box." When it comes to a Cast of Characters list, the witness list is the box.

Here are three examples of thinking outside it:

- You're handling a drug case in which arrests were made in two hotel rooms. The individuals in Room 901 claim to have been unaware of what was taking place in Room 903. Rooms 901 and 903 should make it into your Cast of Characters.
- You're preparing a medical malpractice case in which certain surgical procedures are at the heart of the dispute. These procedures belong in your Cast of Characters.
- You're litigating a trade secrets dispute. The alleged trade secrets should be listed in the Cast of Characters.

Your Cast of Characters should provide one-stop shopping for all the important things in your case. To facilitate this process, you should include a column in your Cast of Characters table that you use to designate the type of thing each player is: person, organization, etc. If you use a word processor to create your Cast of Characters, you can sort the Cast of Characters using this Type column. If you use database software to build your Cast of Characters, in addition to sorting by type, you can use the Type column as the basis for filtering. For example, you could filter your Cast of Characters so that it displays only persons or only organizations.

The Litmus Tests

Your Cast of Characters should be a list of critical things, not every possible thing. For many players, making this call is a no-brainer. For others, a decision won't be so easy. Here are two methods for making a determination.

The Newbie Test: Pretend you're a new staff member who has just joined the trial team. You've been given a weekend to come up to speed on the case. Who are the persons and what are the organizations, documents, and other things about which you should know so you'll look sharp at the team meeting on Monday morning?

The Mentioned in Critical Facts Test: When we say that a person, organization, or other thing is critical to the case, what we're really saying is that there are important case facts that involve this entity. Any person, organization, document, or other thing that you expect to be mentioned in critical facts should appear in your Cast of Characters.

Persons and Organizations

Obviously, your Cast of Characters will include people. Capture the name of each critical person, and an indication of whether they will be a fact witness, an expert witness, or are related to the case in some other way. Also capture the Role-in-Case of each person, in other words, a brief but more specific explanation of why the person is important to the case. The second type of thing to include in your Cast of Characters is organizations. Don't limit yourself to organizations that are parties — list all companies and institutions where key witnesses work or where critical case events occurred. Capture the same type of information that you capture for persons: a Name and a Role-in-Case, an explanation of the connection between the organization and the case.

Include Key Documents & Other Physical Evidence

It's likely that you create a separate Document Index for managing the reams of documents involved in a typical case. Even if you do, your Cast of Characters should include a list of the most important documents in the case. A case may have tens of thousands of documents that you need to manage, but I'm sure you'll agree that only a tiny percentage of these will be critical to the judge and jury. These 50 to 100 key documents should appear in your Cast of Characters. For example, let's say you're working up a contract dispute. The contract that the parties are fighting over certainly belongs in your Cast of Characters. So does the accident report in a personal injury case and the performance review in a wrongful termination case. One way to decide which documents to include in the Cast of Characters is to employ the Mentioned In Critical Facts litmus test. If a document is the subject of important case facts, then list it in the Cast of Characters. Conversely, if a document is not the subject of facts, but rather serves strictly as a source of facts, don't add the document to your Cast of Characters, just deal with it in your Document Index. When you add a document to your Cast of Characters, give it a name and describe its role in the case. In addition to listing key documents, list other important physical evidence in your Cast of Characters. For example, in an automotive products liability case, you should list the parts of the vehicle that are alleged to be defectively designed. Again, capture Name and Role In Case.

Include Key Events

Events in a Cast of Characters? Yes. Now, I'm not suggesting that you turn your Cast of Characters into a Chronology of the day-to-day events in the case. Rather, I'm suggesting that in your case there may be a handful of crucial events — events to which many important case facts will refer. If so, these key events should be listed in your Cast of Characters. For example, in an antitrust price-fixing case, there may be one or more key meetings among competitors during which the price-fixing conspiracy was allegedly hatched. In such a case, it's likely that there are a great many facts that describe the meeting, e.g., when the meeting was planned, who did the planning, when various players arrived, what they did at the meeting, etc. Or let's say that you're litigating a negligent security case in which the plaintiff was mugged in a hotel's parking structure. The mugging is an event that deserves to be in the Cast of Characters. Give the event a name and describe its role in the case.

Include Any Other Critical Thing

Given the nature of the case you are working up, there may be other critical things that deserve to be listed in your Cast of Characters, but which fall outside of the foregoing categories. For example, in a patent infringement case, the ideas claimed in the patent are items that should be listed in your Cast of Characters. And in a slander case against a shock jock, the name of the show on which the alleged slander took place belongs in the Cast of Characters.

Dealing with Jane Doe, John Doe, and Doe, Inc.

In the early stages of a case, it's common to know that some person or persons are involved in the matter, but not yet know their names. Just as we would do if we were filing a complaint against persons unknown, use Jane and John Does as placeholders in your Cast of Characters. This tactic makes it clear that we know important players exist, but we have yet to identify them by name. It turns your Cast of Characters into an aid in the discovery process. Every time you review the Cast of Characters, you'll be reminded that you're missing the names of one or more important players.

For example, in a medical malpractice case, plaintiff counsel knew that one or more nurses were on duty when his client was in the hospital, but he was unsure of their names. He added a J Doe to his Cast of Characters and defined the Role-in-Case as nurse. Don't limit your Doe logic to missing persons. Use this strategy for any important thing that you know is involved in the case, put have yet to discover its name.

Avoid Elaborate Descriptions

It's tempting to use your Cast of Characters to capture the story about each person, organization, or key document listed in it. Many Cast of Character reports I've seen feature a Description column where these details are recorded. Please avoid this practice. It creates a number of problems; the most serious being that you end up with a series of disjointed little stories when what you should have is one overall story of the case. When you enter a description of the case story vis-à-vis a particular player, what are you really doing? You're entering facts — the important case facts that have to do with this player. But important facts belong in your Chronology, not in your Cast of Characters.

Here's another example of the many problems caused by putting facts in your Cast of Characters: Most facts involve multiple players, e.g., "Ryan called Steve and told him to shred the Critical Memo." When you create detailed descriptions of each player, you end up repeating the same fact for multiple players, e.g., once for Ryan, once for Steve, and once for the Critical Memo. And if you have to change anything about the fact, you'll have to find it and edit it in multiple places. If you keep your facts in your Chronology, when something about a fact changes, you only need to edit one item. And when you keep facts in a Chronology, you have one complete story of your case, not dozens of fragmented ones. Each fact lives where it belongs in the overall history of the dispute. Each fact can be independently assessed as disputed or undisputed, good or bad, and so forth. Also note that, if you use database software, there's no downside to moving facts out of your Cast of Characters and into your chronology. Want to focus on the story regarding a specific player? Simply filter the chronology so that it displays only those facts that mention the player of interest.

Show Issue Relationships

Another piece of information to capture about key case players is the case issue or issues to which the player relates. By issue I mean claim or key factual dispute. For example, in a patent infringement case you might have both an infringement and a validity issue. The players involved with the infringement issue are rarely those involved in the validity issue. Linking case players to issues has particular value when you're just beginning the case and the facts have yet to be developed. When you make a link between a witness, organization, or document and an issue, aren't you really saying that there are facts involving that player that will have to do with that issue? And aren't you saying, "I don't know the details yet, but I expect that this witness is going to have a lot to say (i.e., a lot of facts to say) about this issue." Add another column to your Cast of Characters and use it to capture issue relationships. You can capture issue relationships as you first enter players. Or you can forego entering this information initially, and ripple through the Cast of Characters at a later point with your issue-analysis hat on. If you're using database software to create your Cast of Characters, making links between players and issues makes it easy to print Cast of Characters of just those players that relate to a particular issue – a capability that has great value when you analyze your case and develop strategy.

Evaluate Each Member of The Cast

Use your Cast of Characters as an aid when you evaluate your case and as the place to store your evaluations. For your Cast of Characters to be the most useful, you should rate each cast member in terms of criticality and goodness/badness. Once this is done, you can filter your list down from all players to just those that are particularly important or just those that are particularly good or bad. If you're one member of a larger trial team, you can send each litigator a copy of the Cast of Characters and ask them to make an independent assessment of each player. Once done, you can hold a review session to compare evaluations. Comparing evaluations makes it easy to ensure everyone is on the same page or at least has a clear picture of where they agree to disagree.

Capture Questions

As you build your Cast of Characters, you'll no doubt think of questions about various case players that will need to be answered to ensure complete discovery. For example, when you

enter the name of a potential witness, you may realize that you don't even know where the witness lives or works at this point. If you're using word-processing software to create your Cast of Characters, include a column in which you capture these questions. For example, if you had five questions regarding a particular key document, you would list these five questions in the Question cell for the document. If you're using database soft-ware, you may be able to capture your questions separately and link the questions to the player or players they are about. Keeping questions separately eliminates double entry and editing. For example, you only need to enter "When did Ryan and Steve first meet?" once, not twice (once for Ryan and once for Steve). And keeping questions separately means that each can be assigned its own due date and can be independently evaluated in terms of its criticality. Once you build an independent list of questions, you can explore it in many useful ways. You can filter the list of questions down to just those that are about a particular key player. A moment later, you can display a report that lists the most critical questions about all players.

Use Your Cast of Characters To Standardize Naming

When trial teams create case analysis documents such as Chronologies and Document Indexes, it's a common problem to have one person, organization, or document being referred to by multiple names. For example, in an age discrimination case against Rollins Widget Corporation, it wouldn't be surprising to review the Chronology and Document Index and find facts and document descriptions that refer to the defendant as Rollins, Rollins Widget, and RWC. Having multiple names for a single person, organization, or document makes it a nightmare to filter the Chronology or Document Index so it displays any item about Rollins. Your Cast of Characters can help solve this problem. Turn it into a dictionary that lists the preferred name to use for each key entity in the case. Distribute the Cast of Characters to all members on the trial team, and ask them to use the standard name when referring to the person or organization in the Chronology and Document Index.

Begin Immediately

Start your Cast of Characters as soon as you've been retained on a matter. The earlier you start, the more helpful your Cast of Characters will be in determining the people, organizations, and documents about which you need to learn more. Why not start building your Cast of Characters as part of an initial brainstorming session with your client? As your clients tell you who they feel are the key players in the case, you can also get them to tell you the facts of which they're aware with regards to each player. If you start your Cast of Characters early, you can use it as a tool during witness interviews. At a logical point in the interview, give the interviewees a sanitized copy of the Cast of Characters, and have them tell you everything they know about each player. Also have the interviewees tell you what persons, organizations, and documents they feel are missing from your Cast of Characters list.

Create for All Cases

There are many reasons you should make creating a Cast of Characters standard operating procedure — something you do for every case, even those that are "small." We're all familiar with matters that appeared minor but which later turned out to be far more complex than we had first imagined. If you create a detailed Cast of Characters for every dispute, even those that appear small, it's likely that you'll If you start your Cast of Characters early, you can use it as a tool during witness interviews. At a logical point in the interview, give the interviewees a sanitized copy of the Cast of Characters, and have them tell you everything they know about each player. spot potential problems earlier. Further, even small matters have more players than anyone can meaningfully organize and evaluate in his or her head. And the practice gained creating a Cast of Characters for small cases makes you more adept when doing so for larger ones.

Database Software Advantages

Using database software to create your Cast of Characters has numerous advantages over using word-processing software. For instance, database software allows you to enter information using pick lists, thereby saving time and eliminating misspellings. Many database systems allow multiple users to work in a file simultaneously. And some database packages support replication and synchronization. Replication and synchronization permits trial team members to work in separate copies of the Cast of Characters database as they travel, and to merge the changes they make into one updated database file when they re-turn to the office. As I've illustrated in other sections of this article, data-base software also makes it easy to explore your Cast of Characters in ways that are simply impossible using word-processing software. For example, database software makes it easy to filter your Cast of Characters down to any subset of interest. Rather than printing a report that lists every item, print a Cast of Characters that lists only witnesses, or one that lists only those players that you have designated as being extremely critical to the case or particularly good or bad.

Summary

To create a great Cast of Characters, you need to make it far more than a witness list. If a person, organization, document or any other thing is the subject of important case facts, include it in your Cast of Characters. Don't create a detailed description of each player. Instead enter the key facts about each player into your Chronology. Note the issue(s) with which each player is involved. And evaluate your players in terms of both criticality and goodness/badness. These additional pieces of information will make your Cast of Characters a far more useful case assessment tool. Start your Cast of Characters the first day you're retained. And make creating a Cast of Characters standard operating procedure, something you do for every case – big or small. Finally, create your Cast of Characters using a database program. Using a database program instead of a word processor will make the task easier and produce a far better work product.

Hope these have been useful ideas! I would enjoy your feedback.

Greg Krehel is CEO of DecisionQuest's CaseSoft division (www.casesoft.com). CaseSoft is the developer of litigation software tools including CaseMap and TimeMap. He can be contaced at gkrehel@casesoft.com.

Document and Records Management: Understanding The Differences and Embracing Integration

Priscilla Emery

Introduction

Records Management and Archiving practices have become an extremely visible topic in the last year or so. With increasing angst with regard to the safety of both personnel and organisational information and the growing number of investigations into the fiduciary soundness of several notable organisations, such as Enron, Worldcom and others, record keeping has now gained new respect.

Unfortunately, confusion still abounds when it comes to understanding exactly what Records Management and Archiving really is and how it is differentiated from Document Management and other information management strategies. Although, in many enterprises it is recommended that these strategies be linked together, it is still important to understand the differences between them so that key functions and procedures are not overlooked.

Even the word "archive" is used in various ways that can confuse buyers and sellers alike. To some people archive means saving just about everything – to a records manager archive means saving the right things for a specified length of time.

The form that documents and records take has also evolved dramatically in the last several years. More than 10 years ago, when electronic imaging was at its infancy, this writer pointed out that "paper is the symptom – not the disease." The disease is finding the information we need at the right time in order to efficiently address business requirements and to make effective decisions. Unfortunately, the disease has now reached a chronic stage. Paper is still plentiful but e-documents such as word processing files, spreadsheets, photos, video, sound recordings and other unstructured information sources are proliferating across many organisations at an exponential rate. Add to this mix the explosion of e-mail-based documents used as part of the process of enhancing the pace of communication and organisations have the potential to drown in their documents.

Records vs. Documents: Understanding the difference

A document (whether in electronic form or paper) is the basic communication device in what is considered unstructured form (as opposed to structured data records – which in some cases can be embedded within different electronic documents) that is used in most organisations. Document management (DM) systems were and still are developed to provide a library and/or repository where documents can be created, managed, and stored for easier access by departments and users across an enterprise.

Records provide evidence of the organisation, functions, policies, decisions, procedures, operations or other activities of a government agency or corporation or because of the informational value of the data in them. Not all documents are records and records can be both structured and unstructured. Records can be documents but have a more rigorous process associated with managing them. Records can include books, papers, maps, photographs, machine-readable materials, or other documentary materials. They can be created or received in connection with the transaction of public or private business.

Both document management and records management systems have evolved to now support many different types of documents and information. Nevertheless, the reasons for implementing DM systems can be very different from the reasons RM systems are implemented. The value proposition with respect to DM systems is in the sharing of knowledge and collaboration capabilities that can be enhanced by having a document repository in place. Although these capabilities can be part of an RM system as well, RM is more focused on maintaining a repository of evidence that can be used to document events related to statutory, regulatory, fiscal, operational, or historic activities within an organisation. While DM repositories are generally focused on keeping as much as possible for future reference, RM repositories are generally focused on keeping only what is necessary for a specified length of time. An RM system usually deploys a role-based user security model with strict filing permissions for groups of users.

Organisations should have a unique understanding of what needs to be kept as a record, for how long and what needs to be destroyed. This understanding is defined in a file plan. The file plan or what is sometimes referred to as a record plan, groups records on the same subject and allocates record numbers to ensure that related records are either shelved together (or in electronic systems filed together) and automatically assigned a retention schedule. This usually necessitates the development of a thesaurus or taxonomy to categorise records and/or documents in a common and/or standard way.

A well-managed records repository can provide a single point of access to records previously controlled by functional areas or specific individuals and permits access to records throughout their life cycle. Records management systems use automated processes to manage any record regardless of format: paper, electronic, microfilm, etc. The focus of electronic record keeping systems is to preserve the content of electronic records and their context and structure, over time, i.e., a final record should be auditable and locked in its final form. This is somewhat different from generalised electronic document repositories that provide for the checking-in and out of documents that can be revised and unlocked for future revision.

Integration of RM and DM is becoming a reality

In 1999 ***Gartner*** predicted that revenue related to records management functionality would grow from $15 million in 1999

to about $35 million in 2001, much of this growth fueled by government initiatives. At that time Gartner also predicted that by the end of the year 2000, document management vendors would generate more records management-based revenue than the remaining independent records management vendors. Their conclusion is that RM vendors would be hard pressed to compete with the document management (and now content management) vendors that offer the same capabilities and then some. That may or may not have held true in the past few years but what has happened is that the integration of DM and RM features is definitely becoming a necessity for more organisations.

Although many DM vendors are incorporating RM capabilities within their products through interfaces with different electronic record keeping products it is important to note that best practice says any electronic record keeping system should be compliant with the ***DoD 5015.2*** standard or equivalent. This DoD standard is focused on records that are eventually transferred to the ***U.S. National Archives and Records Administration (NARA)***, such as government personnel records, manuals, standards, directives and documents that are scheduled for declassification or redacted items. The ***UK Public Record Office of the National Archives*** has also released functional requirements for Electronic Record Management Systems. Other countries such as Australia and Canada have also identified minimum records management standards for government applications as well. These respective standards are going beyond government confines and are being used across many different industries to set a minimum standard for how records are stored within an electronic repository.

Records are usually required to be saved and archived in their original format so that it is very important for RM systems and the DM systems they may be interfaced with to be able to open any document/record in its original format. Any DM/RM system should create and maintain an audit trail (also called use-history metadata) for all records activity and system functions; and provide access to audit trail information at the fully detailed level (e.g., each individual record access, including record identifier, time, date, and user). The system should provide summary reports of audit trail information (e.g., number of accesses) and track failed attempts of all records activity and system functions.

Diagram One provides an example of how RM and DM can be made to work together.

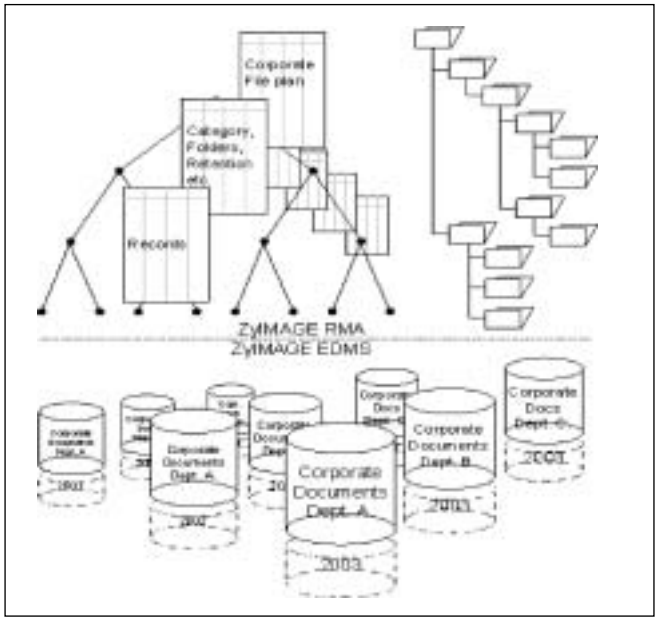


Diagram One: ZyIMAGE Record Management Application

The illustration emphasizes the structured nature of documents in the bottom part of the picture, below the dashed line, with well-organized document repositories. For example, one document repository is created for each department and a new document repository is created each year, therefore, resulting in a two-dimensional grid of document repositories. The system is implemented to enforce this structure defining:

- Exactly which department should record which documents
- What metadata should be used
- How long documents should be kept
- What kind of document identification keys should be used
- Who has access and who doesn't.

The upper half of the diagram depicts the RMA system. On the left, it shows the relational database system that supports the record functions required by RMA standards. On the right, a table of contents is shown which represents a view on all documents based on the records that are stored in the relational database. The role-based security model of the RM system determines which parts of the table of contents are visible to the user and which parts are not.

The RMA system is a separate product that has been developed using the ***Microsoft*** .NET framework. The application is a scalable multi-tier application that is entirely web enabled. The server that is running the RMA layer may be the same server that is running the database layer but may also be run on (multiple) different servers. A group of users may be assigned to a specific RMA layer to balance the workload and increase the performance. The system is scheduled for DoD 5015.2 certification in May 2004 where it will be tested using a Microsoft SQL-server database.

Users need to be on the lookout for suppliers that are compliant with the DoD 5015.2 standard while at the same time providing an architecture for handling the long term viewing requirements associated with ever-changing electronic document types, such as being able to view, JPEG, TIFF, PDF, Microsoft Word and others.

Any DM or RM system should provide a sufficiently powerful range of search features and options. These might include: wild-card or exact-match searching, proximity or adjacency searching, relevance ranking of search results, use of stop-words, limits on maximum size of results set from a search, query by image content, or others. These systems should allow for searching on metadata, record content, or assigned subject categories (using a controlled vocabulary – thesaurus, categorisation scheme, taxonomy, etc.). They should also ensure that all access privileges (permissions and restrictions) are enforced on all retrievals.

According to Gartner's Rita Knox, "As a data interchange representation, XML will be long-lived, ensuring longer-term usability for the RM applications that use it. (1) Using XML databases versus flat files or relational models is one way that ZyLAB has designed its products for the future. But just using XML is not enough to ensure optimum performance on large repositories of information. ZyLAB uses its ZyINDEX full-text indexing engine to index every piece of information in the XML repository. This activity combined with the use of its unique fuzzy search engine provides not only optimum performance versus traditional database searching methods, which require that specific fields be indexed and identified at the beginning of an investigation, but also provides for the flexibility of adding new information and having it indexed and searchable as the investigation grows.

1. Knox, Rita, ***Gartner Research Note,*** "Records Management Needs Metadata and XML," March 14, 2003

2. Complete certification planned for May, 2004

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

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

IRMA PRESENTATION – 7 SEPTEMBER 2004

Evening session presented by
Ross Palmer (MIIA, FIIA, CISA), Computer Audit Manager, Hogg Robinson plc

"COMPUTER AUDIT BASICS – 2: AUDITING THE INFRASTRUCTURE AND OPERATIONS"

In Derek Oliver's "Computer Audit Basics – 1", he addressed, among other things, two essential factors of the computer audit process:

1. that all auditing should be undertaken on the basis of risk; and
2. that all risks should be business related, because at the end of the day, that's what matters.

The areas of control identified as important in mitigating the effects of business risks are likely to include a large proportion associated with information technology. In particular, the effectiveness of controls to ensure the confidentiality, integrity and availability (CIA) of information – an organisation's greatest asset after its staff – will be critical to its survival, and possibly to that of its suppliers and customers.

Arguably, nowhere are CIA controls more important than in the area of computer infrastructure and operations, which covers such diverse issues as strategic/operational IT decision-making, asset classification and network management protocols.

This session will attempt to outline the areas of computer audit focus for reviewing infrastructure and operations with particular reference to industry best practice and some of the emerging areas of regulatory and governance concern.

There may even be a spark of wit to keep it lively. After all, humour is essential in a job where 50% of the salary should be considered "danger money" (and thus tax-free).

Portable Computing Device Security

Didi Barnes

1. Preface

1.1 Scope

To provide a proprietary standard document covering Portable Computing Device (PCD) security (see definitions) in order that this may facilitate in the production of policy, best practice and training documents thus assisting companies in securing such devices.

1.2 Definitions

PCD: means "Portable Computing Device" and should be taken to refer to a PDA, laptop or any other device capable of carrying or processing data, so may also include certain cellular telephone and other devices that technological advances make available.

PDA: means "Personal Digital Assistant", and will be used when specifically referring to handheld devices, such as Palm OS or Windows CE devices.

External memory: should be taken to mean any removable, portable memory device, e.g. USB flash drives, CF (Compact Flash) cards, SD (Secure Digital) cards, memory sticks and any other similar memory device.

POCKET PC: this term should be taken to mean the Windows CE operating system since it is used synonymously when describing that operating system.

WLAN: Wireless Local Area Network.

WEP: Wired Equivalent Privacy: a type of encryption used for wireless data streams.

1.3 Caveats

Didi Barnes and First Base Technologies can accept no responsibility for any consequences should you decide to use the information contained in this paper. Whilst various software and hardware are mentioned in this document, this should not be taken as a recommendation of that software and/or hardware.

2. Introduction

Emphasis should be placed upon the fact that the contents of this document can apply to any Portable Computing Device ("PCD") so is as applicable to laptop PCs as PDAs and other handheld devices. The context will make clear if an element of this text applies to a specific type or brand of PCD.

Hardware constraints previously limited PDAs to being glorified personal organisers, thus laptop PCs have been for many years the portable business tool of choice. However, rapid advances in PDA technology leading to enhanced functionality, such as faster processors, greater storage capacity and wireless communication technologies, are now resulting in these devices being deployed as full-blown business tools in the corporate environment. Their ease of portability is likely to result in their superseding laptop PCs for many environments, heading towards a future of seamless, cable-less connectivity between devices, between people and between networks.

Consider the data a PCD or external memory device (e.g. USB flash drive, CF and SD cards, etc) can carry. PIM[1] information, e.g. address book, calendar, to-dos, notes; all of which can be exploited for the purposes of social engineering, identify theft and to verify identify, e.g. when requesting a password be reset [7]. These devices can contain network connection information providing an attacker with a neat backdoor into the organisation. The other data such devices can contain is merely limited by memory capacity, which is becoming increasingly less an obstacle. That data could be trade secrets, CRM information, personnel data, patient records; all having potentially serious repercussions in the wrong hands.

Even given all this, according to a survey commissioned by access control firm, Pointsec Mobile Technologies, a third of employees leave such business information and access details unprotected on their PDAs [4]. Even if they do have basic security enabled on their devices, these controls may be able to be bypassed by a determined attacker. Whilst many companies have become aware of the particular security issues surrounding the portable nature of laptop PCs and have made due provision for these in their security policies, other PCD devices and associated external memory tend to be overlooked. Their small size has a psychological "out of sight, out of mind" effect. So what then, of the risks?

Device-level risks: As it becomes more difficult for attackers to breach security controls of networks and PCs due to rising awareness and thus better security, attackers will be looking at other ways to bypass these security boundaries. PCDs, particularly PDAs, and external memory cards will become an increasingly attractive target; theft and other compromises will thus become more likely.

Communication-level risks: most PCDs nowadays have one or more wireless technologies, e.g. 802.11x, Bluetooth, IrDA, built-in. Those that don't, usually have facility to attach hardware to implement them externally, e.g. via a CF Bluetooth card, or a PCMCIA 802.11x card (a PDA may require a "sleeve" or "expansion pack" to take a PCMCIA card). Each of these technologies carries its own set of risks, for example the risk of

[1] PIM = Personal Information Management

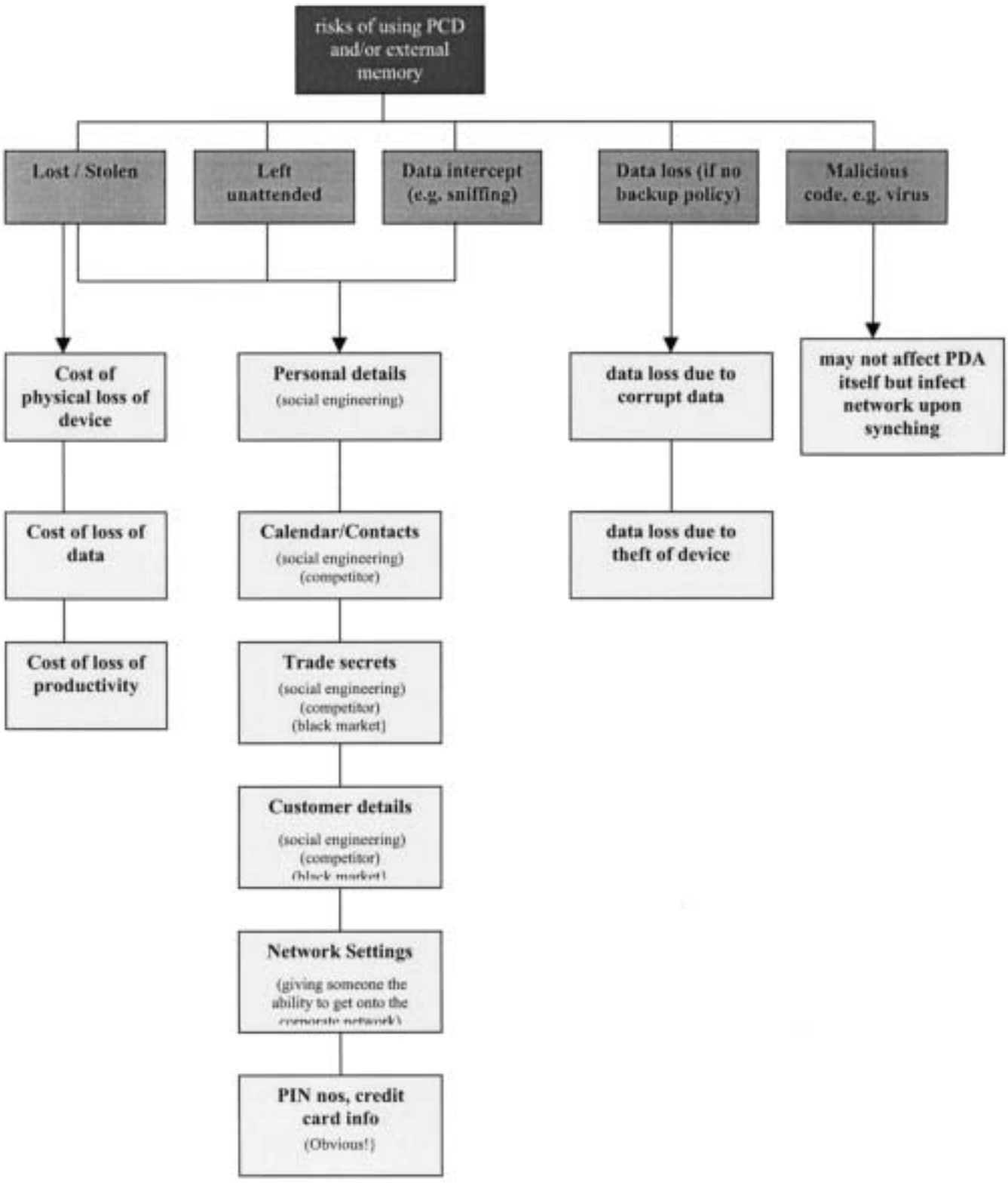
data capture over the air by traffic analysis (sniffing), the risk of connections being made with unauthorised devices, and other exploits.

Companies urgently need to implement a suitable security policy to address these issues. Staff awareness and training campaigns should be implemented. If users know the risks and how to ameliorate them, this will provide an excellent first layer of security. Disaster contingency plans should be made should a device or its data fall into the wrong hands.

To conclude this section, the big question to ask is: ***Q) "what would the impact be on our organisation if the device, external memory devices, data contained on them or being transferred via networks - got into the wrong hands?"***

This question, and ideas to reduce the vulnerabilities associated with it, will be explored in the remainder of this document.

3. Risk Analysis



4. Security Policy Checklist

The right-hand column contains cross-references to more detailed information that can be found in the next section.

PCD policy should take into account wireless, homeworking, remote access, backup, anti-virus and windows security policies.	5.1
PCDs should be forbidden without prior authorisation	5.2
Only authorised PCDs are permitted to connect to the network	5.2
Train staff how to spot and document suspicious activity / rogue PCDs	5.2
Those authorised to use PCDs should receive training prior to their issue	5.2
Only company-owned PCDs should be authorised, privately owned devices and external memory should be prohibited.	5.2
PCDs should be used for business-use only – no personal data / software	5.2
Users should not be allowed to install software, change settings on their PCD	5.2
Define documentation procedures should security be breached	5.2
Ensure personnel know the value of data and the risks if it gets into the wrong hands	5.2
Purchase PCDs that offer the best security options	5.3
Define responsibilities for deploying, installing and managing PCDs	5.3
Employ a method of patch and update management for PCDs	5.3
Standard-build should be mandatory for all PCDs	5.3
A user should not usually be an administrator on the PCD	5.3
Check regularly for rogue PCDs	5.3
Check regularly that PCDs continue to conform to security policy	5.3
Employ some form of asset-tagging on PCDs	5.4
Don't allow owner information to be displayed on the PDA (i.e. "owner information" settings).	5.4
Use external locking facilities, e.g. Kensington lock, where possible	5.5
PCDs should be kept locked away when not in use and external memory stored separate from the PCD.	5.5
PCDs should be kept in a way as to obfuscate them, e.g. not in an obvious looking laptop case, for example	5.5
PCDs should be used out of public view (if possible) and kept out of public view as much as possible.	5.5
PCDs should preferably never be left unattended, if they are, they should be locked away.	5.5
Laptop PCs should be configured in a way as to take account of operating system security, e.g. Windows 2000 security policy	5.6
Laptop PCs should employ BIOS, boot and hard disk passwords	5.6
All PCDs should have unnecessary services, ports and devices disabled.	5.6
PCDs should have OS and application settings set in a way as to maximise security.	5.6
Enable audible alarms on PCDs where possible to alert the user to e.g. someone trying to connect.	5.6
Use a third party access control package, preferably one that offers biometric or picture-based access controls; don't rely on the device's access controls	5.6
Use software that provides a "logic bomb" in order to wipe data should access controls be breached, if feasible for your organisation.	5.6
Consider all data carried on PCDs and external storage as sensitive, however innocent it may seem.	5.7
Choose a suitable disk / file encryption tool and ensure personnel know via policy and training which data should be encrypted. Audit that they are using encryption and are remembering to use it for external storage as well.	5.7
Communications devices should be kept disabled between uses, e.g. disable Bluetooth.	5.8
Decide what communications technologies are authorised and disable those that aren't or remove the device.	5.8
Users should be within eyeshot of one another if doing peer-to-peer networking and initiate the connection by verbal request first.	5.8
Use a product that can help prevent unauthorised synching.	5.8
Change the default settings to secure communications devices; refer to our papers on wireless and Bluetooth to assist with this.	5.8
Have a different network logon to the device logon, preferably different to the one you'd use on your desktop and in a different user group with different policy.	5.8
Use external authentication if possible, e.g. RADIUS	5.8
Treat all PCDs as untrusted where possible, especially devices using wireless, they should be firewalled.	5.8
Consider using two-factor authentication to protect access to web-based resources.	5.8
Encrypt network / connections settings where possible, certainly avoid having passwords on the device, users should enter them manually.	5.8

Use a Secure VPN solution for protecting data in transit, especially if over wireless networks.	5.8
Consider using MMIS[2] or similar	5.8
Decide which policy you are going to have for external memory and ensure users adhere to it	5.9
If external memory is allowed, it should be kept separate from the PCD when not in use	5.9
Make sure your encryption policy covers external memory	5.9
Privately-owned external memory should be banned	5.9
Use a personal firewall, e.g. Zone Alarm on a laptop, eTGuard Pocket PC on PDAs.	5.10
Use anti-virus software and have an update policy	5.11
Implement a backup / synchronisation policy	5.12

5. Security Policy Guidelines

5.1 Introduction

Please note that the software mentioned in this document is described in more detail and has links provided in Section 6.

A security policy is a legal document that empowers you to take action if any of its rules are broken – you can't enforce what you don't have!

The next few pages give more detailed background to the checklist on the previous page, to assist with writing a suitable policy for PCDs. However, it should be noted that such policy needs to take into account related policies, some aspects of which may not be given in much detail in this document, such as:

- Wireless and network security policy
- Windows security
- Anti-Virus policy
- Backup policy
- Home-worker and mobile networking policy
- Remote access policy

5.2 General Usage Policy and Staff Awareness and Training

Many of the aspects below are considered in more detail later in the document. This is intended to be a guideline to policy specifically relating to personnel, and to staff awareness and training aspects.

All personnel:

Devices not allowed: Personnel should be informed that any PCD (PDA, laptop computer, and any other type of portable computing device which may emerge onto the market) are not allowed within the vicinity[3] of the organisation without prior and written authorisation. They should also be informed that connecting to any networks with any devices other than devices they are authorised to use (e.g. their desktop PC) is forbidden.[4] These points should also be written into the employee induction process and contract of employment. It should be clearly stated the disciplinary action that would be taken should they breach these regulations.

Suspicious activity: Personnel should also be informed that PCDs may be used to launch attacks on the organisation and should be required to document any "suspicious" activity. For example, personnel should be trained to be suspicious of someone outside or inside the building walking about with a PDA or laptop – is that person authorised or is perhaps hacking the network? Such staff awareness could avert a large number of attacks launched via wireless or wired networks if policy-makers thought to include this angle in their training.

Those personnel authorised to use a PCD:

Such personnel should be given (or informed where to find) copies of corporate policy pertaining to PCDs, and related policies. They should be given training upon issuance of such devices and only granted permission to use a device once they have been "signed off" as having received the appropriate training. This training should cover the items below (which should also be included as part of policy anyway):

Only business-owned devices should be authorised: privately owned devices and external memory should be forbidden (it is difficult to enforce controls on privately owned devices).

How to use the device: upon issuing a device, users should be trained how to use it from a general productivity perspective. This will avoid users wasting time by not being productive, and avoid accidental security breaches, through not knowing how to do something, e.g. connect using Bluetooth and their mobile phone. This may also include training them on how to use individual applications and how to perform such tasks as synchronisation and file encryption, for example.

General Security Awareness: users should be made aware of the security risks surrounding using and carrying PCDs and external memory. They should be educated as to the value of data – many personnel just don't think about the value or significance of the data they are carrying, if they did, they would probably instinctively take more care.

Software/data: no personal data or programs should be allowed. Policy and training should state who is authorised to install software or change settings and what data is permitted to be on a PCD/memory card, for example. If someone has permission to install software, they should ensure it is approved software before installing it. Passwords and credit card numbers, etc., should not be stored on the PCD. All this may require tailoring to notional groups of personnel, e.g. some personnel may be allowed to add software, others may not, some people may be allowed to use e-mail and remote access, others may not. The aim of all this is to reduce the chance of applications/data/settings being added or changed, which may otherwise compromise security.

External memory: you need to decide if this allowed at all. If it is, you need to decide how it should be used as per the above and ensure to include this in policy and training. Policy should state that all such memory should be handed in for secure destruction if it fails. See section 5.9 for further details.

[2] MMIS = Microdoft Mobile Information Server

[3] "vicinity" because the presence of a WLAN will circumvent the 'obvious' physical boundary of your organisation/premises.

[4] As to the above, if it is stated they are not allowed to connect this clearly covers if they try to connect to a WLAN (for example) outside the physical area of your building, e.g. in the car park.

Encryption and other security controls: personnel should be made aware of encryption, access control (e.g. password) and anti-virus policies. They should be given the appropriate training to ensure they know how to conform to these policies.

Backup policy: users should be informed – and shown – how to ensure their device is backed up to avoid the risk of data loss (for example through device failure or theft). They should be informed of the synchronisation policy (which may just be all – or part of – backup policy for PCD devices). They should be trained how to implement this part of policy.

General security: Users should keep their ownership of a PCD obfuscated (section 5.4). Your policy and training should include physical security issues such as how a PCD should be secured when not in use. The training should, for example, include a demonstration of how a Kensington lock should be used (see section 5.5).

Documentation: Define documentation procedures for employees to follow if they discover a breach in security, e.g. inform a particular contact name and backup contact/s name/s immediately a device is lost or stolen. This should also include recording suspicious activity (see "suspicious activity" under "all personnel" above).

Enforcement: should state that users should follow the appropriate security policies and should define how users are to use their devices in order to facilitate device, data and connections protection. They should be told that failure to follow policy could result in recall of the device, possibly dismissal.

5.3 Deployment and Management of Devices

Following on from the previous section, below are pointers for policy for administrators themselves, rather than users. There are many software tools available to facilitate many of these requirements, see section 6.

Purchase of devices: administrators should ensure that there is a standard for the brand of equipment and attempt to ensure that only equipment that a) offers the best security options and management options, and, b) is compatible, is purchased.

Responsibilities: who will be responsible for installing and managing the devices and for patches and upgrades.

Asset tagging: should be employed. See section 5.4.

Standard build: should be mandatory, based upon thorough testing of what software and settings are required. The standard build should also include a) additional access control software (see 5.6), b) encryption software (see 5.7) and c) anti-virus software (see 5.11). There is cloning software available to help in putting standard builds onto PDAs (see section 6). Care should be taken to configure settings as part of the standard build specification in such a way as to maximise security.

Limit user rights: preferably, a user should not be a local administrator on the device. Only administrators should be enabled to install and deploy devices and change settings. Users should not be allowed to make changes to standard build, e.g. by adding their own software. If certain users are allowed to add software to their device, policy should state that they should only install authorised software. Use of permissions and user/groups can be used to limit what a user can do. This will mean that you can keep control of the device – and therefore its security.

Checks for rogue devices: administrators should regularly perform checks, as part of policy, to ensure that only authorised personnel have PCDs. This could be implemented by ensuring that heads of departments or supervisors know who is and is not allowed such devices and to ask them to paper any unauthorised devices. They should be informed that evidence of an unauthorised device may be the presence of a synchronisation cradle at someone's work area, as well as someone using a PCD. This method should enable rogue devices to be identified and removed before a more serious security breach occurs. Such devices are often those that through poorly configured security or lack of awareness of the owner, have the greatest potential to breach security.

Checks for security: administrators should check devices on a regular basis to ensure that the devices continue to conform to policy, e.g. settings have not been changed, or programs added which may compromise security. They should interview users to ensure that they are continuing to use devices according to policy – people get lazy.

(Details of tools that can assist with many of these processes may be found in Section 6).

5.4 Asset Tagging

All PCDs should be tagged, their details and those of the user recorded on a database. This will facilitate speedy identification of unauthorised "rogue" devices, which will be those not documented on the asset register. It will also assist in the safe return of devices should they fall into the hands of an honest person. It will also assist for insurance purposes should the device be permanently mislaid or stolen.

Kensington sell a tracking device called "CompuTrace"[5] which enables tracking and recovery for laptop PCs, as well as motion detector alarms. Such products may be useful in that they can, with use of appropriate stickers on the device, act as a deterrent to all but the most determined attacker. There are likely to be such products available for a PDA.

Australian Projects sells a product called "STOP anti-theft system" (http://austprojects.com.au/stop.htm) which provides a numbered identification plate beneath which lies an indelible registration number and a "stolen equipment" warning. They also provide a red warning sticker, which can be affixed to the device. Again this is a deterrent but since there are still a lot of honest people about, such a technique will enable an honest person to record a mislaid device that can then easily be tracked to its rightful owner.

A company called Idstrip.com (http://www.idstrip.com) provides labels with an identifier that identify the machine to that company should the finder phone the number on the label.

A related issue is whether or not to have owner information on the device. If someone obtains unauthorised access to a PDA, they can use such information for social engineering. In addition, depending on the company name that is showing, it may make it even more tempting for a potential attacker to find a way to subvert the device than if the owner information didn't exist or had something trivial such as "brain" on it. Whilst owner information can be useful to enable a device to be returned to you if it goes missing, it is better to rely upon some form of asset tagging service as the means to get the device returned.

[5] http://www.kensington.com/html/1145.html

In this case, you would make it part of policy to forbid users to enter owner information. If this really cannot be done, then at least untick the "show information when the device is turned on" box within the "owner information" settings (Windows CE)[6].

5.5 Physical Security

Policy could include the following, for example:

Locks: Kensington or other locking devices should be used when possible and appropriate, in order to secure the device to a fixture or fitting that is not easily moved. It is perhaps surprising that people will loop the cable around something that can be easily lifted up - users need to be made to think about what they are doing.

Whilst there are not so many ways currently on offer to secure PDAs compared with laptops, this is likely to change due to demand. Currently, Kensington offer a lock for certain brands of PDA that attaches to the stylus slot (www.kensington.com) and Force (http://www.force.com/) sells a product called "The Bond" which they describe as compatible with Palm III, Palm IIIX, Palm VII, IBM WorkPad PC and Symbol SPT-1500 devices.

General best practice: these tend to be based on obfuscation and not leaving a device unattended without due care:

- Devices should be kept locked away when not in use, and a Kensington and/or Bond device (see previous page) should be employed where possible.
- When travelling, devices should be transported in a way such as to obfuscate them. It is preferable to avoid using an "obvious" looking laptop or other case. This very simple technique would avoid many of the thefts that occur!
- Devices should be kept out of public view as much as is possible – if someone sees you have one, they might begin thinking about ways they could steal it or connect to it! If possible, if a device needs to be used, the user should go somewhere private to use it and keep it locked away when not in use.
- PCDs should never be left unattended. Devices should not be left in cars, for example. If a device must be left in the hotel room, it should be locked in the hotel room's safe. If the item is too big for the safe, it should be locked in a case (preferably not an "obvious" looking laptop case) and hidden from view; perhaps hidden behind a chair and locked to a central heating pipe for example. External memory cards and other external memory devices should be removed and kept with the person in their wallet or purse and kept in a place separate from the device that uses it.

5.6 Access Control

Laptop computers

Laptops should be dealt with using the same security policy as desktop PCs but with even more vigilance due to their portable nature. For example, suitable password policy, NTFS or Linux file permissions, turning off shares, disabling guest accounts, enabling a good lock-out policy, not displaying last user, disabling unnecessary services and ports, etc. Don't let the user have administrative rights. In addition, BIOS passwords, boot passwords and hard disk passwords should be employed. Preferably, only the administrator should know the BIOS password – then only they can access the BIOS to make changes. It would be good – if possible – for the user to have a username and password different from the domain logon used on their desktop. A disk encryption product should be used for sensitive data and additional access controls, if necessary.

PDAs and other such devices

PDAs will have one of the two major operating systems for PDAs: Palm OS (Palm Pilot, Sony and Handspring Visor) or Windows CE "Pocket PC" (Compaq and HP Ipaq, Casio, etc.). There are some PDAs such as the Sharp Zaurus that run on a Linux and Java™ platform too, and much guidance on the Web as to how to convert an Ipaq (for example) to the Linux platform.

Basic measures: such operating systems have similar problems to conventional operating systems. Basic measures are disabling unnecessary ports, services and devices and disabling communications services between usage.

Change default settings: default settings do not generally offer adequate security. All application and operating system settings should be checked and changed where necessary before deployment of devices, to ensure the device offers the maximum protection.

Audible alarms: Enabling whatever audible alarms are available can be useful (or make use of software that provides them). If an alarm is set to go off if the device is being tampered with, a request for data transfer is received, etc., the user will be alerted (if they are near enough to hear it!) and hopefully in time to prevent a security breach. There are motion detectors available for these devices, for example.

There are a number of password crackers on the market for Palms, e.g. www.palmgear.com ("Sword") and www.freewarepalm.com. Most likely there are also password crackers for Windows CE in the same way that there are for Windows (e.g. L0phtcrack, LC4 etc.). This means that the default access controls are not sufficient protection. It is highly recommended to employ a more comprehensive and secure solution via third party software, preferably a biometric or picture solution.

If it would be catastrophic if the data got into the wrong hands - you should consider using the type of access control that offers "logic bomb" capability which will wipe all the data on the device should access controls be breached. It is also advisable to enable audible alarm functions should access controls be breached.

Examples of access control software available are:

Biometric fingerprint readers: For example Authentec (http://www.authentec.com/) is a biometric fingerprint reader that can fit on the handheld.

Biometric hand writing recognition software: though it should be noted that if an attacker has found a document with the user's signature, they may be able to copy this and log on anyway. Some products allow a password to be used in addition to the signature, which provides an extra level of security. Or users can use a word other than their signature as their biometric logon. Examples are:

- CIC Sign-on;
- KeCrypt also provides encryption solution;
- PDALok;
- Safeguard PDA

[6] Note that even if the "show information" box is unticked, the basic details such as name, company and phone number will still be shown on the "today" screen anyway.

Picture-based access controls: two types:

- Those that allow access upon selection of the right combination of thumbnail images, e.g. Pointsec for Pocket PC and Safeguard PDA.
- Those that, through using a stylus to touch certain points of a picture, allow you to obtain access, e.g. Visual Key.

"Logic Bomb" Software: that will wipe data from the device should access controls be breached. This facility is optional in certain software such as the military grade PDA Defence.

5.7 Disk / File Encryption

It is advisable to keep all data encrypted on a PCD, however "innocent" it may appear. Whilst the data may not be sensitive in the classic sense, it may contain information that can be exploited for social engineering purposes as previously mentioned. Thus the safest approach is to consider all data as sensitive. However, this is unlikely to be feasible in a large organisation, but encryption of sensitive information should be a minimum requirement and policy should clarify what should be encrypted and the type of encryption to use.

128-bit encryption should certainly be used as a minimum and there are a number of products that can fulfil this requirement, either as their whole function or part of an access control solution. See section 6 for examples of such software.

5.8 Data Communications

There are various factors to consider when reviewing risks and potential vulnerabilities surrounding data communications. These can relate to laptop PCs as well as to handheld devices:

Unauthorised use of device: if someone obtains access to your device via theft, for example, and it has an account on the network and perhaps other settings such as WLAN, dial-up, etc., it may mean that person has an account on the network. Such unauthorised access to a PCD may thus result in a network compromise, not just a device compromise.

Unauthorised connections: unauthorised pairing of devices, for example.

Synchronisation: connecting via a cradle to your local PC/laptop/corporate network carries its own set of potential vulnerabilities.

Wireless connection (e.g. 802.11x) to e.g. a hotel WLAN for purposes of using their Internet connection, or connecting to a corporate WLAN for using the network, which may include using the Internet, synchronisation, browsing and using network resources for example.

Dial-up when "on the road", using e.g. a Bluetooth, IrDA or cable connection to a GSM device (e.g. cell phone) which acts as the intermediary for using the resources of the Internet via the GSM device. Or via conventional dialup using a modem card connected to a hotel's telephone system, for example.

Security Guidelines:

- Employ methods to reduce chance of loss or theft (see section 5.5);
- Decide which technologies are permitted and disable those that are not;
- Educate users to disable communications devices when not in use (e.g. if not using wireless, disable wireless adapter);
- Users should, where possible, verbally request a connection before making it and be within eyesight of one another (e.g. particularly relates to Bluetooth). This can help reduce the chances of unauthorised connections, not least because if it is policy that someone wanting to connect should ask first, if a connection request comes in and the person has not been asked, it can be assumed that the connection request is perhaps unauthorised. This is just another idea to add a layer.
- Use a product which can as part of its access controls (see section 6) prevent unauthorised synching via password protection;
- Users might not understand the significance of just pressing "ok" if they get a connection request they are not expecting. They should be informed of the risks and to click "no" if in any doubt whatsoever. [2]
- Change the default settings within communications services, which usually do not provide sufficient levels of security, e.g. enable 128-bit WEP (for 802.11x);
- Don't store passwords on the device - untick any "remember password" boxes. This will require passwords to be manually entered each time, but will make it much harder for an attacker to use the device to attack your network.
- Disable "allow other devices to connect to me" (WinCE, may be different for Palm OS), and use encryption and suitable pairing passwords, etc;
- Have a network logon different from the device logon. Users frequently get set up on the domain with an "easy to enter" password because it is a nuisance to enter a long password onto a PDA. However, "easier to enter" equates to "easier to guess", thereby compromising the security of the entire domain! Preferably use an external authentication method e.g. RADIUS or DigiPass.
- Treat all PCDs as untrusted, especially PDAs and any devices using wireless technologies, and only allow them to connect via a firewall;
- Consider using a two-factor authentication solution to protect access to web-based resources, e.g. RSA Mobile;
- Encrypt network / connection settings where possible and use a Secure VPN solution or something similar for protecting data in transit, especially over wireless network connections;
- Consider using Microsoft Mobile Information Server (MMIS) or similar (see section 6).

5.9 External storage

This is worth a section all on its own, due to its significance as far as security is concerned. Memory sticks, CF (Compact Flash) cards, USB flash drives and other external memory devices are small and somehow psychologically not associated with the serious data they may be carrying. This can lead to carelessness - the small size of such external memory lends them to be easily mislaid or stolen.

Users should be educated that such memory should be considered as important as the device that utilises it, and that it may actually be more valuable than the device itself, depending on the nature of the data contained within it!

There are three philosophies concerning deployment of external memory:

a) **Keeping data on external memory only:** meaning that users are not allowed to store data on the PCD itself. This

primarily relates to PDAs, unless you consider having removable hard drives for your laptops using this same philosophy. In this situation, a user keeps all data, therefore reads/writes to, the external memory device which, when the PCD is not in use, is removed and kept separately from the PCD (e.g. in the user's wallet). This is, of course, analogous to keeping a cheque card separate from cheques. If the PDA is stolen, so long as the card has been removed, there will be no valuable data on the PDA. You could then purchase PDAs with just enough non-volatile memory to store programs, which could help reduce the chances of data being written to the PDA. Of course, encryption should be used for data, whether it is on the PDA itself or the external memory.

b) **Banning use of external memory completely:** in this case, the thought is that users won't be using – and perhaps losing or having stolen – external memory. To facilitate this approach, PDAs would need to be purchased that have sufficient internal memory for programs and data and, in addition, preferably purchase devices that don't have the facility for attaching external memory.

c) **Keeping some data on external memory, some on PCD:** this may be essential, for example where a PDA does not have the internal memory to cope with demand. However, policy should dictate what, and what not, to store on external memory, and the encryption policy surrounding that data. Users should be educated on the value of external memory. They should be informed that that they are not allowed to store personal data or programs on the external memory (in the same way as they aren't on the PCDs themselves). They should also be informed that privately owned external memory devices are forbidden.

5.10 Personal Firewall

A personal firewall should be employed on all PCDs, e.g. Zone Alarm for laptops and desktops. There are personal firewall and IDS systems emerging for PDAs, but these are somewhat limited at the moment. It seems that CheckPoint may have one on offer.

5.11 Virus and Malicious code – AV Policy

The rest of this section will refer specifically to PDAs, because it is likely that laptop PCs use the same AV policy as desktop PCs, although this should be checked!

Viruses that have been directed towards the PALM OS are PalmOS.Liberty.A, PalmOS.Phage.A, PalmOS.Vapor.A. There do not seem to be any targeting Pocket PC … yet[6].

The hardware constraints imposed on PDAs tend to mean that the operating system[7], and many of the applications that have been designed to run on them, are stripped-down versions of those that run on conventional PCs. This also means that such programs have weaker security than their PC equivalents. It may be that boundary checking has been eliminated in some areas, so facilitating the potential for buffer overflow attacks. [2]

Whilst PDAs haven't been a target for malicious code attacks so far, that is likely to change as such devices become more commonplace and attackers realise the potential of exploiting them. Meanwhile, one of the major concerns is the ability of PDAs to act as transport vectors for malicious code onto the corporate network. For example, were a user to open an e-mail attachment that contained malicious code (e.g. a virus) on their PDA, whilst the malicious code may not affect the PDA itself, it could be carried onto the corporate network upon synching.

Thus, as with any other type of computer, it is important to implement some form of anti-virus policy on PDAs. There are two types of virus scanner for PDA:

a) **Local:** those that run on the PDA itself. F-Secure's Anti-Virus for Pocket PC is an example of such a scanner, which scans e-mails as well as files loaded onto the PDA. Updates are pushed to the device from the user's PC or may be downloaded via a wireless connection. There needs to be policy for how updates are handled and the frequency with which a user should obtain them. Note that the volume of AV identities may give a problem with memory on some devices.

b) **Remote:** the identities sit on a server (e.g. the machine to which the PDA is to be connected for synching). When the PDA (client) connects for synchronisation via a PC or directly onto the network, it connects to a server which scans the PDA before any infections can occur. McAfee's "VirusScan PDA" is an example of this type of scanner, which scans PDA files upon synching. However, Sophos say that if their product is installed on the desktop, its on-access scanner will detect any viruses transmitted when the PDA or mobile phone synchronises with the desktop PC" – so it may be that having a good desktop solution is enough…

5.12 Backup Policy

Your policy should state how backups should be implemented.

If the device is used for manipulating data, rather than just referencing it (i.e. where it is contained elsewhere) backups should be carried out at least once a day. Thus your backup policy will really be dictated by the way in which devices are used.

If a member of staff is out in the field, then hopefully they will have a laptop PC with which to synchronise their device. If not, perhaps they could use an external memory card for backing up data (and keep the card separately from the PCD, as mentioned previously).

It may be that synchronisation is the way in which backups are performed, therefore synchronisation policy will be synonymous with backup policy. If this is the case, staff should be informed that this synchronisation process provides the only way of backing up their data, then they will take more care about doing so!

See section 6 *(overleaf)* for details of backup tools.

[7] Windows CE, for example is a stripped down version of W95 with a few applets added [5]

6. PDA Software

This section attempts to give a good overview of software tools that are currently (Sept 2003) available for PDAs. The software is listed in alphabetical order under each category.

Handango (http://www.handango.com/) is one of the best resources for PDA software on the web. Much of the software listed below is available from there …

6.1 Encryption & Access Control Products

Some of the below offer both Encryption and Access Control, others offer each as stand-alone features.

CIC Sign-on http://www.cic.com/products/signon/	Their site says, "…is the first log-on security utility for handheld organizers that uses biometric signature verification to keep the data on your device safe! Sign-On will allow you and only you to gain access to the data on your organizer. Just sign your name or create a personalized drawing or design and Sign-On will verify your signature or personalized design to unlock the device."
Cryptinfo http://www.cryptinfo.com/cryptinfo/index.shtml	Their site says, "CryptInfo is a secure password manager for the Palm and the PC. Securely store your passwords, credit card numbers, and more! Synchronize your information between your PC and your Palm device. Your privacy is protected with strong encryption technology that scrambles your information so that only you can see it!"
Digipass for Pocket PC http://www.vasco.com/products/product.html?product=24	Their site says, "Many Pocket PC devices have wireless connectivity capabilities, relying on WAP, GPRS or similar technologies. With such connected Pocket PC's, Digipass provides strong user authentication and digital signatures for over-the-air mobile commerce transactions." "Multiple profile support is one of the many features of the Digipass for Pocket PC. It allows more than one virtual token on one Pocket PC, each with its own secret key for access to different servers, networks and web sites."
F-Secure FileCrypto™ http://www.f-secure.com/products/filecrypto/	Their site says, "…protects stored data from unauthorized access. The solutions are strong, automatic and transparent to the end user."
Handango Security Guard™ http://www.handango.com then search for it.	The site says, "a robust enterprise-class security tool that enables file and folder encryption …this application secures data and controls application access…168-bit encryption…" Note that Handango have many other security products available too.
Kaspersky® Security for PDA	See anti-virus software section.
KeCrypt http://www.kecrypt.com/home.htm	Their site says: "KeCrypt – as unique as your signature KeCrypt's unique patented technology is the world's first to offer genuinely effective security based on new biometrics and PKI technology".
Microsoft Mobile Information Server http://www.microsoft.com/miserver/	This supports standard isecurity protocols, e.g. VPNs, WTLS[8], SSL, PPTP and supports hop-by-hop encryption and IPSec encryption between MIS Enterprise Edition and MIS Carrier Edition. Can help secure data in transit and can also manage how user' use their devices, i.e. which applications need security.
MobiPassword™ http://www.mobipassword.com/	Their site says "MobiPassword is a multi-platform Personal Identification organiser, providing an all-in-one solution for the security, mobility and automatic use of your personal identification information." "… the only application featuring automatic matching of login names and passwords to their place of use."
movianCrypt™ http://www.certicom.com/products/movian/moviancrypt.html	Their site says "movianCrypt™ integrates a password-based user log-in system with strong encryption technology to achieve data security on your Palm OS or Pocket PC device …transparent to end users…automatic encryption."
PDA Defense™ *(previously known as "PDA Bomb")* http://www.pdadefense.com/enterprise.asp	Their site says "the industry standard in PDA data security, provides multi-layered security for Palm, Pocket PC and Blackberry devices." "With its high level of security [it is] being used within all branches of the military, the White House, the FBI and civilian enterprises throughout the world." It lets administrators mandate security settings and push them to a PDA upon synchronisation. It also provides data wiping if access controls are breached.

[8] WTLS = wireless transport layer security

PDALok http://www.pdalok.com/	Their site says, "PDALok™ is security software added to your Pocket PC that restricts access to unauthorised users unless a live signature from the rightful owner is presented. It locks it from access or from synchronisation, so all data held on your Pocket PC is fully protected.
PDASecure Enterprise http://www.trustdigital.com/prod16c.htm	Their site says that the product offers "centralized managed security, database encryption, sync protection, beam protection, wipe password, configurable by end user and administrator, single-key encryption, 3DES, AES, you can select specific applications to protect, directory integration with NT Domain, ODBC & LDAP." They also offer a range of other products "each addressing a unique area of need in total security architecture."
PGP Mobile http://www.pgp.com/products/enterprise/mobile.htm	Their site says: "PGP Mobile for Palm OS devices provides capabilities similar to PGP Disk for secure data storage and PGP Mail for secure messaging. PGP Mobile for Windows CE provides the secure-messaging capabilities of PGP Mail for Pocket PC devices, allowing PGP Mail-compatible messages to be sent and received securely. PGP Mobile also syncs PGP-specific information such as key-rings between Windows computers and handheld devices." However, different options are available for Palm OS compared to Windows CE.
Pointsec for Pocket PC http://www.pointsec.com/solutions/	The list of features on their site says "Real-time encryption, removable media encryption, media encryption policy, enforceable mandatory access control, Picture PINTM authentication, QuickPINTM authentication, central administration with Pointsec profiles, user account lockout, authenticated ActiveSync, user transparent encryption, remote help, XTNDConnect management abilities".
SafeGuard PDA http://www.utimaco.de/eng/indexmain.html	Their site says: "… a powerful solution to protect your [PDA] and the data stored on it against unauthorised access." "... Innovative authentication mechanisms such as biometric signature recognition or Symbol PIN offer optimal user convenience, the strong encryption protects your data while stored or in transit over the Internet, the centrally enforceable security policy keeps your environment consistently protected."
Secure Star – various encryption products http://www.securestar.com/	Their site says, "The leader for real-time hard disk encryption" and they do many such products.
Sentry 2020 http://www.softwinter.com/sentry_ce.html	Their site says "…enterprise security tool utilising transparent encryption…128-bit, operates at the volume level so is faster…" The site also has other useful PDA tools as well.
Visual key http://www.viskey.com/	This is a picture-based access control product where access will only be allowed if certain previously defined spots in the picture (one of theirs or one of your choice) are clicked upon in the correct order. Palm OS and Pocket PC are supported and there is a PC version too – a really useful product.

6.2 Anti-Virus Products

avast! 4 PDA Edition http://www.avast.com/i_idt_155.html	Their site says that this product is not due for release until summer 2003. It announces the product as being "… designed to protect pocket devices (PDA) from viruses. The importance of PDAs is growing every day, and so these devices are likely to be a target of virus attacks rather soon. As their connectivity gets better and better, such an attack is easier to do" and says both Palm OS and Windows CE are supported.
F-Secure Anti-Virus for Pocket PC http://www.europe.f-secure.com/wireless/pocketpc/pocketpc-av.shtml	Their site says "…is an anti-virus software solution that runs locally on the pocket PC device. It provides up-to-date and always available protection…since the solution runs on the mobile device, it is able to detect and delete also all malware that enters the device through wireless connections."
Kaspersky® Security for PDA http://www.kaspersky.co.uk/buyonline.html?info=971980	Their site says: "…a comprehensive approach to anti-virus protection of data stored on PDAs, as well as information transferred via PC or extension card." It also "protects against unauthorized access to data stored on PDAs as well as secures access to the portable device itself using a password system. The ability to block access to PDAs running Palm OS for fixed time periods."
McAfee's VirusScan™ Wireless http://www.networkassociates.com/us/products/mcafee/antivirus/remote_user/vs_wireless.htm	Their site says: "McAfee® VirusScan™ Wireless, the first member of the McAfee Wireless product family, is a comprehensive virus security solution for mobile and handheld devices, such as PalmPilots and PocketPCs, that connect to your network. As millions of users turn to powerful, pocket-sized devices, the threat of infection through PDAs increases. VirusScan Wireless is a comprehensive way to guard against this threat. "

Sophos http://www.sophos.com/products/sav/	Their site states that, "The threat of viruses infecting PDAs and mobile phones has been widely hyped by some anti-virus companies. However, it is possible for PDAs to carry a virus into a company (thus avoiding any email gateway protection), and for the suspect file to be copied onto your desktop from the PDA. Sophos Anti-Virus protects against this kind of infection through its on-access scanner, detecting any viruses transmitted when the PDA or mobile phone synchronises with the desktop PC."
Symantec AntiVirus for Handhelds http://ses.symantec.com/products/products.cfm?productid=237	Their site says: "… Palm OS and Pocket PC compatible … deployed and installed to the desktop and then automatically transferred to the handheld device during synchronization … Wireless and synchronized LiveUpdate™ support ensures up-to-date virus definitions for the handheld. In addition, synchronized LiveUpdate™ enables simultaneous enterprise-wide deployment of virus definitions to desktops using Symantec AntiVirus Corporate Edition."

6.3 Backup

Pocket Backup http://www.spritesoftware.com/products/pocket_backup_plus.html	Their site says: "backup directly to your host PC or a Network using the convenient PC Agent. You can backup when connected via ActiveSync or any form of wireless networking (Win XP and Win 2000 only). There is a lot of other functionality – see their site for details.
CF card Backup http://www.handango.com then search for it	Handango's site says: "CF card Backup for Pocket PC 2002 Card Backup Tool lets you quickly and easily backup your Pocket PC memory data to a memory card. Backed up data can be used to restore your system should it start to malfunction due to some data error. Card Backup Tool can let you choose to save ALL Files or PIM Files only. Card Backup Tool can let you choose the Saving Place before Backing up or Restoring it. Select the Saving Place.(Built-in Storage or CF card Storage)."

6.4 Network Analysis and Administration Tools

AirScanner Mobile Sniffer http://www.handango.com and search for it	Note such a product could be used in conjunction with the "mini" version of the well-known NetStumbler, and other similar software. Handango's site says: "As a network administrator, you want to protect your users' confidential data. What better way to do this than to stroll down the hall with Airscanner™ Mobile Sniffer hidden in your pocket? Thanks to our support for Ethereal packet capture format, grabbing your user's passwords out of the airwaves is as easy as watching a movie! Your users unintentionally send their passwords through the air in clear text, so it is better that you discover this first before a malicious drive-by hacker does it for you. Airscanner™ Mobile Sniffer also works in promiscuous mode, so you can also discover unauthorized users who may be associating with one of your access points."
Backbone Software NT Services http://www.handango.com and search for it	The Handango site says "… a web based tool for Microsoft windows server administrators that need to monitor, access and edit windows services from remote locations using a pc, pda or a smartphone". "… Administrators can easily browse their way through workgroups and computers to get an overview of the running, stopped and disabled services on any computer in their network, view detailed information about the computers eventlog, View, start, stop and restart IIS websites, backup IIS metabases, reboot remote servers/workstations, kick/logoff/disconnect terminal service users, kill hanging processes and more.
iAdmin Mobile 2002 http://www.jrbsoft.com/solutions/iadminmobile.asp	This tool lets you remotely manage your "Windows NT/2000 or XP infrastructure right from the palm of your hand" so it is different from the other tools in that it is not a tool to manage PDAs, but a tool for administrators to manage their network! Of course such tools can be used for illicit purposes, so it is useful to point out that they exist!
PE Explorer Suite 2003 http://www.handango.com and search for it	Handango's site says it is the most powerful explorer for Pocket PC, can help manage zip files, browse and manage network resources "will fulfil all your file management needs, whether they reside locally, remotely on FTP server or remotely on your windows network."

Pocket Controller Enterprise http://www.handango.com and search for it	A powerful tool which offers "remote manage and support mobile devices from a central location. Connect to remote mobile devices using Wired or Wireless TCP/IP LAN/WAN, ActiveSync, modem or cellular connections. Support for direct connections or through HTTP, SOCK4, or SOCK5 proxies. Create administrator and user accounts, allow/deny privileges, allow users to accept/reject remote control session requests, configure authentication and encryption settings. It can also view the remote file system or to transfer files to remotely view or edit the registry of remote devices, provides audit logging, printing features, remote DOS box and much more" according to Handango's site.
PocketLANce http://www.pocketlance.com/	A "unique" tool for browsing, managing and transferring windows network resources from pocket PC, can work via ActiveSync connection or via RAS or DUN, it integrates with standard File Explorer on Pocket PC and supports different network access rights and security levels with an optional peer-to-peer operation mode."
z2 PocketLAN http://www.handango.com and search for it	Handango's site says: "… a dedicated network software, main features: enable network folder in pocket file explorer, auto scan remote computer names and browse, open remote computer files, auto detect network connection, reconnect to network resource when it is available, etc.
PocketMySQLAdmin for Pocket PC http://www.handango.com and search for it	Handango's site says: "Connect to a MySQL database server anywhere in the world, maintain multiple Database server profiles, perform full queries and view results, select, update, insert, delete and all other MySQL supported queries supported by the software. Create and delete databases and tables, password protected interface, add delete and modify user rights, works with MySQL version 3.X onwards and supports all Pocket PC PDAs.
Pocket Nanny http://www.handango.com and search for it	Very useful tool that Handango describes as "… an application designed to assist an IT department lock down their deployed base of Pocket PC based devices, so only desired applications can be used."
PortTrakker http://www.handango.com and search for it	Handango's site says: "PortTrakker is the most feature rich and comprehensive TCP/UDP Port Database available for the Pocket PC."
Sprite Clone http://www.spritesoftware.com/products/sprite_clone.html	Their site says "Sprite Clone simplifies the deployment of Pocket PCs across an Enterprise. Set up one Pocket PC, capture a complete image of it, which includes the file system, databases and registry, and deploy this image to your target Pocket PCs." so a very useful tool.
TigerSuite PDA http://www.tigertools.net/tt2kpda.htm	Their site describes it as "Network Security Assessment Software plus network tools" and says "includes modules for remote scanning, service detection, penetration testing, network and file tools such as a hex editor, IP subnetter, host collaboration and remote Trojan scanner with remediations. The suite operates from Main Memory or Storage Card and is compatible with wireless, IrDA and LAN internet and/or network connections."

7. Bibliography

[1] Roberto Di Pietro and Luidi V. Mancini. Security and privacy issues of hanheld and wearable wireless devices. In Communications of the ACM (September 2003/Vol. 46. No. 9.

[2] Roberta Bragg. Protect your PDAs, PDQ! MCPmag.com (February 2003).

[3] John Phillis. Recommendation for a Security Utility to protect Palm organisers.

[4] John Leyden. PDA security slackers, the lot of you. In The Register (9 September 2003).

[5] Brian M. Posey MCSE. PDA security with Windows CE. In TechRepublic (April 29, 2003, 08:46 BST).

[6] Dave Croxton. PDAs in the Corporate Environment. In Sans reading room. (Sept 5, 2001)

[7] Richard Price. The PDA as a Threat Vector. In SANS reading room. (March 2003).

[8] Nelson Beach. Handheld Security: A Layered Approach. In SANS reading room.

[9] Darrin Murriner. Pocket PC – Secure or Unsecured? In SANS reading room. (2001)

Didi is a partner of First Base Technologies and its lead consultant for wireless and remote access. She is also responsible for Research and Development and has produced a number of white papers. For more information, check out www.fbtechies.co.uk. For more information, contact Didi Barnes at First Base Technologies: 01273 454525 or at info@firstbase.co.uk.

BCS MATTERS!

Colin Thompson, BCS Deputy Chief Executive, reviews some of the current BCS news items.

The New BCS Membership Structure

Much attention has been paid in this column and elsewhere to the membership grading changes over the past two years as we planned the changes to the Society's Charter and byelaws. Against that background it is good to be able to report that the planning is now over and the Charter was duly launched on 1st May. The formal launch event took place at the Salvador Dali Gallery on London's South Bank on 29th April with enthusiastic support from UK government representatives in the form of Sir Peter Gershon, until recently the Head of the Office of Government Commerce, and Lord Sainsbury the DTI Minister.

It is too early to declare the project a total success but the early signs are very encouraging. At the time of writing (25th May) it is clear that the intake of new professional members in the first month of the new regime will be at least double the total number for the ***whole of the previous year***. Our target is to recruit at least 10,000 new professional members during the course of the coming year – a target which now looks a good deal more achievable than it did when it was originally set.

A major element of the success of the first month has been the **Trusted Source** campaign. Nominations from existing BCS professional members now total almost 2000, all of whom have been invited to join the BCS at the level of MBCS and we are currently piloting arrangements under which existing Fellows will be able to nominate the most senior and eminent members of the profession for entry at the FBCS level. In addition, we are in discussion with more than 20 companies with a view to establishing *Trusted Source* arrangements for their staff.

One of the main benefits of these *Trusted Source* arrangements is that they enable us to complete membership processing very rapidly. The objective is to complete the necessary processing within three days of an application. That is a challenging target but we are now hitting it on a consistent basis.

Those who enter under these *Trusted Source* schemes do not generally obtain Chartered status at the point of entry – although they may of course apply as soon as they are admitted. There is however one exception to this rule; those who join under the arrangements agreed with IBM recently will enter as full Chartered Professional members with the right to use the post nominal letters CITP and the title *Chartered IT Professional*. The agreement with IBM follows a full mapping of the company's professional structure against the BCS Industry Structure Model and the accreditation of the associated processes by the Membership Committee.

Although IBM is currently the only company within these arrangements, we hope to add others during the course of the coming year. The scheme is open to others who are able to meet BCS requirements in respect of the necessary professional structure and the associated processes.

A change of name for the ISM

After 20 years, the BCS Industry Structure Model has had a name change. The latest version of the model bears the label *SFIAplus*. SFIA – the *Skills for the Information Age* framework is owned jointly by BCS, IEE, IMIS and E-Skills and is the UK's leading high level skills framework. The two products are closely related and are generally complementary, the ISM providing a more detailed view of the skills identified in the SFIA framework. However, the naming differences and a number of differences in the structuring served to hide that relationship and to confuse the marketplace. So, with the need to update the ISM as the foundation for a new family of BCS development products, we have taken the opportunity to change both the label and the structure to establish full compatibility with SFIA.

New Development Products

The first products in a new line of development tools for both members and employers were launched shortly after the main launch of the new BCS. The coincidence of timing is part of a deliberate strategy designed to ensure that we are seen by these two main constituencies as delivering services that are relevant and valuable.

For BCS members, the new products will include full on-line access to SFIAplus. That facility was not available with the ISM – indeed to gain access to the model members had to buy a full copy. The new service, *Browse SFIAplus*, will be supported by a range of tools, packaged as *Career Manager* which will enable members to identify their development needs and to define an appropriate course of action. The activity undertaken as a result can then be recorded as part of the individual's Continuing Professional Development (CPD) record. This is a sophisticated, integrated system developed with the assistance of software developers *Infobasis* which will provide a much higher level of development support to members than in the past and which represents an approach to CPD based much more on facilitating meaningful development than in simply recording development activity undertaken.

For the Employer community, the new products include *Skills Manager* launched on 6 May and *Career Developer* scheduled for delivery later this year. As with the individual member products, those for the corporate market are browser based and a built on the common platform of SFIAplus.

Skills Manager is designed to enable IT organisations to identify and to manage their IT skills so that business requirements are matched against people skills. The products uses a skills inventory within which the skills and specialisms of all IT staff are matched against the external standards within SFIAplus and configured to the organisational structure and skills profiles of the particular business. The organisation is then able to analyse skills gaps and to identify the skills required for particular projects.

Career Developer will complement Skills Manager and is aimed at organisations that want to go beyond identifying and managing their IT skills to provide integrated career development planning. The product will enable the organisation to:

- Set up, record and manage cycles of training and development.
- Assign roles, such as participant, supervisor or mentor.
- Automatically generate an individual's development objectives and actions.
- Provide detailed development analysis and progress reports.

Skills Manager and Career Developer will be supported with both consultancy and training services and BCS will provide fully supported and accredited development schemes similar to the long-standing Professional Development Scheme.

BCS Submits Evidence on Identity Cards

The BCS has submitted detailed comment to the Home Affairs Committee Enquiry into Identity Cards. As might be expected, these relate mainly to technical and practical concerns rather than to the political issues associated with the proposals. Major concerns identified by BCS include the following:

- The lack of any firm and fixed statement of what the system is meant to achieve, what success or failure criteria are imposed and which scope limitations have been imposed – all of which adds risk to the (already high) level inherent in large systems.
- Difficulties for those who are disabled, incapacitated, infirm or otherwise incapable of handling the complexities of an identity card .
- Reduced data privacy resulting from proposals for the release of personal information in certain circumstances.
- Proposals to exempt children until they reach the age of 16 – when reliable identification is much more difficult than at birth.
- The difficulty for some people to provide required biometric information – including those who are disabled, house-bound or institutionalised together with some of those in remote rural communities.
- The fact that biometric data, whilst highly accurate, is not infallible.

BCS and the Royal Academy of Engineering report on Complex IT Projects

Billions of pounds are wasted every year on new IT systems, according to a new report published by the BCS and the Royal Academy of Engineering. Despite many examples of good practice, the report says, there is still a lack of professionalism in software engineering that could even be dangerous in safety-critical systems. Britain is failing to produce software engineers and managers with the IT and project management skills to commission and execute complex IT projects.

The report provides detailed analysis both of the reasons why complex IT projects fail and of the resultant waste of resources. The extent of that waste is staggering. The UK public sector alone has spent an estimated £12.4 billion on software in the last year and the overall UK spend on IT is projected to be a monumental £22.6 billion. The team looked at a range of studies showing that only around 16 per cent of IT projects can be considered truly successful – a figure that would, even on the basis of a conservative estimate, put the cost of such failures into tens of billions of pounds across the EU.

And Finally…

Back to where I started with the launch of the New BCS and a quote from Sir Peter Gershon at the launch event which, in just a few words, very neatly encapsulates the case for professionalism and professional qualifications in IT.

'I can't' he said ' think of another engineering area where such a low percentage of people belong to a recognised professional institute or have a recognised professional qualification.

'If I ask an architect and civil engineer to design an unsafe bridge their professional integrity and competence will make them say they won't do it. But if in all innocence I ask a software architect and engineer to design an unsafe system - unsafe because there is inadequate time for testing - how often do we hear those professionals saying no, not at any price, in that timescale?'

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)

HUMOUR PAGES

Below is an actual letter sent to a Bank. The Bank Manager thought it amusing enough to have it published in the Guardian newspaper in the UK.

Dear Sir,

I am writing to thank you for bouncing my cheque with which I endeavoured to pay my plumber last month. By my calculations some three nanoseconds must have elapsed between his presenting the cheque and the arrival in my account of the funds needed to honour it. I refer, of course, to the automatic monthly deposit of my entire salary, an arrangement which, I admit, has only been in place for eight years. You are to be commended for seizing that brief window of opportunity, and also for debiting my account £50 by way of penalty for the inconvenience I caused to your bank. My thankfulness springs from the manner in which this incident has caused me to rethink my errant financial ways. You have set me on the path of fiscal righteousness. No more will our relationship be blighted by these unpleasant incidents, for I am restructuring my affairs for the future, taking as my model the procedures, attitudes and conduct of your very bank. I can think of no greater compliment and I know you will be excited and proud to hear it. To this end, please be advised about the following changes: I have noticed that whereas I personally attend to your telephone calls and letters, when I try to contact you, I am confronted by the impersonal, ever-changing, pre-recorded, faceless entity which your bank has become. From now on I, like you, choose only to deal with a flesh-and-blood person.

My mortgage and loan repayments will, therefore and hereafter, no longer be automatic, but will arrive at your bank, by cheque, addressed personally and confidentially to an employee at your branch whom you must nominate. You will be aware that it is an offence under the Postal Act for any other person to open such an envelope. Please find attached an Application Contact Status which I require your chosen employee to complete. I am sorry it runs to eight pages, but in order that I know as much about him or her as your bank knows about me, there is no alternative. Please note that all copies of his or her medical history must be countersigned by a Notary Public, and the mandatory details of his/her financial situation (income, debts, assets and liabilities) must be accompanied by documented proof. In due course I will issue your employee with a PIN number which he/she must quote in dealings with me. I regret that it cannot be shorter than 28 digits but, again, I have modelled it on the number of button presses required to access my account balance on your phone bank service. As they say, imitation is the sincerest form of flattery. Let me level the playing field even further by introducing you to my new telephone system, which you will notice, is very much like yours. My Authorised Contact at your bank, the only person with whom I will have any dealings, may call me at any time and will be answered by an automated voice service: Press buttons as follows:

1. *To make an appointment to see me.*
2. *To query a missing payment.*
3. *To transfer the call to my living room in case I am there.*
4. *To transfer the call to my bedroom in case I am sleeping.*
5. *To transfer the call to my toilet in case I am attending to nature.*
6. *To transfer the call to my mobile phone if I am not at home.*
7. *To leave a message on my computer, a password to access my computer is required. Password will be communicated at a later date to the Authorised Contact.*
8. *To return to the main menu and to listen to options 1 through 9.*
9. *To make a general complaint or inquiry.*

   The contact will then be put on hold, pending the attention of my automated answering service. While this may on occasion involve a lengthy wait, uplifting music will play for the duration of the call. This month I've chosen a refrain from "The Best of Woodie Guthrie: Oh, the banks are made of marble, with a guard at every door, and the vaults are filled with silver, that the miners sweated for."

   On a more serious note, we come to the matter of cost. As your bank has often pointed out, the ongoing drive for greater efficiency comes at a cost which you have always been quick to pass on to me. Let me repay your kindness by passing some costs back. First, there is a matter of advertising material you send me. This I will read for a fee of £20 per page. Inquiries from the Authorised Contact will be billed at £5 per minute of my time spent in response. Any debits to my account, as, for example, in the matter of the penalty for the dishonoured cheque, will be passed back to you. My new phone service runs at 75p a minute. You will be well advised to keep your inquiries brief and to the point. Regrettably, but again following your example, I must also levy an establishment fee to cover the setting up of this new arrangement.

May I wish you a happy, if ever-so-slightly less prosperous, New Year?

PROGRAMMING PROVERBS

Don't get suckered in by the comments — they can be terribly misleading. Debug only code.

It is easier to change the specification to fit the program than vice versa.

Technological progress has merely provided us with more efficient means for going backwards.

The First Rule of Program Optimization: Don't do it. The Second Rule of Program Optimization (for experts only!): Don't do it yet.

If the code and the comments disagree, then both are probably wrong.

Steinbach's Guideline for Systems Programming Never test for an error condition you don't know how to handle.

All programmers are playwrights and all computers are lousy actors.

"What's that thing?" "Well, it's a highly technical, sensitive instrument we use in computer repair. Being a layman, you probably can't grasp exactly what it does. We call it a two-by-four."

If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization.

If it works, don't fix it.

There is always one more bug.

The number of bugs present in a software package is directly proportional to the number and importance of the people present at the first public demonstration.

There comes a point when the process of fixing one bug creates at least two more bugs. There's never time to do it right, but there's always time to do it again.

"A programmer is a person who passes as an exacting expert on the basis of being able to turn out, after innumerable punching, an infinite series of incomprehensive answers calculated with micrometric precisions from vague assumptions based on debatable figures taken from inconclusive documents and carried out on instruments of problematical accuracy by persons of dubious reliability and questionable mentality for the avowed purpose of annoying and confounding a hopelessly defenseless department that was unfortunate enough to ask for the information in the first place."

REAL PROGRAMMERS

Real Programmers don't write specs - users should consider themselves lucky to get any programs at all and take what they get.

Real Programmers don't comment their code - if it was hard to write, it should be hard to understand.

Real Programmers don't write applications programs - they program right down on the bare metal. Applications programming is for feebs who can't do systems programming

Real Programmers don't eat quiche - in fact Real Programmers don't know how to SPELL quiche. They eat Twinkies and Szechwan food.

Real Programmers don't write in COBOL. COBOL is for wimpy applications programmers.

Real Programmers' programs never work right the first time. But if you throw them on the machine, they can be patched into working in 'only a few' 30-hour debugging sessions.

Real Programmers don't write in FORTRAN. FORTRAN is for pipe-stress freaks and crystallography weenies.

Real Programmers never work 9 - 5. If any Real Programmers are around at 9am it's because they were up all night.

Real Programmers never write in BASIC. In fact no programmers write in BASIC after the age of 12.

Real Programmers never write in PL/1. PL/1 is for programmers who can't decide whether to write in COBOL or FORTRAN.

Real Programmers don't play tennis or any other sport that requires you to change your clothes. Mountain climbing is OK and Real Programmers wear their climbing boots to work in case a mountain should suddenly spring up in the middle of the machine room.

Real Programmers don't document. Documentation is for simps who cannot read the listings or the object code.

Real Programmers don't have an honours degree from UMIST, don't go to hep parties where people sit around talking about their first program. Real Programmers don't drive flash cars, use CB rigs or have heart stickers on their sandwich boxes. All that stuff is for people who would like to be Real Programmers but couldn't make the grade.

THE 8 LAWS OF PROGRAMMING

1. Any given program, once it is running correctly, is obsolete.
2. Any given program costs more and takes longer.
3. If a program is useful it will have to be changed.
4. If a program is useless it will have to be documented.
5. Any given program will expand to fill the available store (and the rest).
6. The value of a program is inversely proportional to the weight of the output produced.
7. Program complexity grows until it is beyond the capability of the programmer who maintains it.
8. Make it possible to program in plain English, and you will find that programmers cannot write plain English.

Member Benefits Discounts

Mark Smith

We are pleased to announce that we have recently extended our range of benefits to include discounts on events that are likely to be of interest to our members. We have secured a 20% discount off the Risk Management Congress 2004 (www.iir-conferences.com), which takes place on 7th and 8th July this year in London. Unicom have also kindly offered us 20% off all their events and training courses, see www.unicom.co.uk for the wide range that they offer. Finally, the Compsec 2004 business security event takes place on 14th and 15th October. There is already a £200-off early bird offer, but IRMA members can take advantage of this discount right up until October! Contact details for all of these discounts are below:

Software

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

Events

Event	*Discount Negotiated*	*Contact*
Compsec 2004 (www.compsec2004.com)	£200 off the full price	Jane Macmillan [janemacmillan@tinyworld.co.uk]
Computer and Internet Crime 2005 (www.cic-exhibition.com)	15%	Paul Webster [paul@panpres.co.uk]
Risk Management Congress 2004 (www.iir-conferences.com)	20%	Sindi Chong [schong@iirltd.co.uk]
All Unicom events (www.unicom.co.uk)	20%	Julie Valentine [julie@unicom.co.uk]

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

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)

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

BCS
THE BRITISH COMPUTER SOCIETY

Management Committee

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 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	Wal 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
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

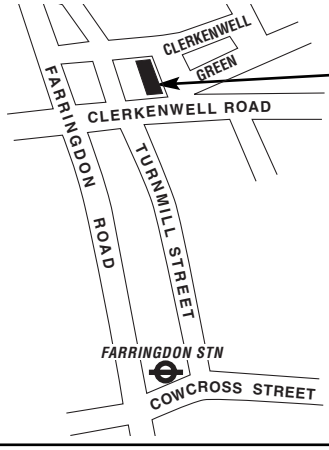
Administration

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

Venue for Full Day Briefings



Old Sessions House
Clerkenwell Green
London EC1

KPMG
8 Salisbury Square
London EC4

Venue for Late Afternoon Meetings