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

JOURNAL

volume 15 number 4 winter 2005 ISSN 1741-4229

40th ANNIVERSARY YEAR, 1965-2005

Programme of Briefings & Meetings 2005/2006

Title	Meeting type	Date
IS Governance and Anniversary celebration	Full day briefing	Tuesday 18 October
Mobile Computing (Joint meeting with IT Faculty)	Full day briefing	Thursday 24 November
2006		
Computer Audit Basics 4: Application Controls	Late afternoon meeting	Tuesday 24 January
Control Aspects of ITIL (Service Delivery) / Cobit	Late afternoon meeting	Tuesday 07 February
System & Data Integrity / Securing Your Infrastructure	Full day briefing	Tuesday 07 March
Wireless Technology	Late afternoon meeting combined with IRMA AGM	Tuesday 02 May
Project Control – The Auditor's Role in IS Projects/Systems Development	Half day briefing	Tuesday 06 June

Apart from the Joint Meeting with the IT Faculty, all meetings are proposed to be held at BCS, 5 Southampton Place, London WC2
This is a draft programme only and is subject to change. For confirmation of dates and further information,
watch the **Journal**, email **admin@bcs-irma.org** or visit our website at **www.bcs-irma.org**

The late afternoon meetings are free of charge to members.
For full day briefings a modest, very competitive charge is made to cover both lunch and a full printed delegate's pack.
For venue map see back cover.

Email distribution is coming . . . . .

Beginning from the first issue in 2006, IRMA is moving from paper to electronic distribution of the Journal, so we need your email address! If you have not already supplied it, please can you send your email address to our admin office at admin@bcs-irma.org with your membership renewal or to the chair at brewer.alex@gmail.com (preferably with the subject "IRMA contact details"). Many thanks.

Contents of the Journal

GUIDELINES FOR POTENTIAL AUTHORS

The *Journal* publishes various types of article.

Refereed articles are academic in nature and reflect the Group's links with the BCS, which is a learned institute governed by the rules of the Privy Council. Articles of this nature will be reviewed by our academic editor prior to publication and may undergo several iterations before publication. Lengthy dissertations may be serialised.

Technical articles on any IS audit, security, or control issue are welcome. Articles of this nature will be reviewed by the editor and will usually receive minimal suggestions for change prior to publication. News and comment articles, dealing with areas of topical interest, will generally be accepted as provided, with the proviso of being edited for brevity. Book and product reviews should be discussed with the appropriate member of the editorial panel prior to submission. All submissions should be by e-mail and in Microsoft Word, Word-Pro, or ASCII format. Electronic submission is preferred.

Submissions should be accompanied by a short biography of the author(s) and a good quality electronic digital image.

Submission Deadlines

Spring Edition	7th February	Autumn Edition	7th August
Summer Edition	7th May	Winter Edition	7th November

PLEASE NOTE THE EMAIL ADDRESS FOR

IRMA ADMIN IS:

admin@bcs-irma.org

The views expressed in the Journal are not necessarily shared by IRMA.
Articles are published without responsibility on the part of the publishers or authors for loss occasioned
in any person acting, or refraining from acting as a result of any view expressed therein.

Editorial Panel

Editor
John Mitchell
LHS Business Control
Tel: 01707 851454
Fax: 01707 851455
Email: john@lhscontrol.com

Academic Editor
Dr George Allan
University of Portsmouth
Tel: 023 9284 6425
Fax: 023 9284 6402
email: george.allan@port.ac.uk

Phil Kelly
Liverpool John Moores University
Tel: 0151 231 3838
Email: p.kelly1@ljmu.ac.uk

BCS Matters
Colin Thompson
British Computer Society
Tel: 01793 417417
Fax: 01793 480270
Email: cthompson@bcs.org.uk

Events Reporter
Rupert Kendrick
Tel/Fax: 01234 782810
Email: RupertKendrick@aol.com

Australian Correspondent
Bob Ashton
Wide Bay Australia Ltd
Tel: +61 7 4153 7709
bob_ashton@excite.com

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

John Mitchell

The military are trialling the use of RFID tags to help identify its assets and to reduce the incidents of friendly fire (an oxymoron only slightly worse than 'military intelligence'). For 'assets' read: machinery, vehicles, weapons and wetware (people). You can imagine the scene as an American F22 swoops down on a truck in the desert. 'Confirming identification of truck . . . Oh, oh, it's one belonging to the Brits and its got six special forces guys on board and they are all wearing Calvin Klein boxer shorts'. Now think of the problem faced by of one of our chaps dressed in mufti in order to infiltrate a terrorist cell. 'Okay Siddique, scan him with the RDIF reader. Well, well, a nice pair of M&S socks under that well worn robe, please step into this nice little room . . .'.

At the moment the military test versions (much more rugged than the civilian equivalent apparently) require 4 AA batteries to power them, so a battery failure reverts you to potential enemy status. Perhaps there is an opening here for a wind-up version as part of the army's BCP? 'Keep cranking trooper. You are the only thing between us and oblivion'. The downside scenarios are endless: a faulty batch of chips, power failure, duplication, substitution, forgery, poor data base administration, interface failure, etc. The whole RFID thing is something that we need to get to grips with quickly. We need to identify the risks and assess the controls. Once again the technology appears to be moving ahead of our ability to control it. as it has done so many times during the forty years that IRMA has been in existence.

One of the amazing things about controlling the technology over the last four decades is that the underlying principles of confidentiality, integrity, availability and compliance have remained unchanged. Sure the technology has moved on, but this has not negated the underlying methodology for assessing the risks. We can control the technology and manage the people. These are not quite the same thing. We manage people by implementing policies, standards and procedures, but until we can implant a chip we are still unable to control them. That is what makes auditing so fascinating. It is not the computer that steals the money, but a person. A computer does not carry out a denial of service attack unless subverted by a person. The abnormal program abend is caused by the programmer, not the program. So people management is really important and that is one reason why I argue that security is a human resource challenge. After all it is HR that conducts the background check. It is HR that sets the employment policies and staff review processes and it is HR that drives the termination process. All in all, it is a pretty solid case for HR driving security. Indeed, perhaps the chief security officer should be part of HR? It is certainly worth opening the debate.

Last month we provided a free full-day technical briefing for our members as a way of celebrating our fortieth anniversary and you can see some of the photographs from that event elsewhere in this edition, together with a letter from Fred Thomas who was a previous Treasurer of the group. You will also find an interesting paper by John Leach on Threat Based Security Engineering, another from a team at Portsmouth university on development risks, a report from our current chairman Alex Brewer, a down-under column from Bob Ashton and an update on our parent body from Colin Thompson.

Remember, this is the last printed edition of the Journal. Next year we go fully electronic so we need your email address. A move into the electronic age after forty years. Is that progress, or what?

The compliments of the Season to you all from your Management Committee.

Chairman's corner

Alex Brewer

Merry Christmas!

Or 'Happy Holidays' if you prefer! The Christmas edition of the Journal is now upon us. At the time of writing I'm wondering about the Christmas shopping. Perhaps you are thinking of asking for or buying some shiny new devices for Christmas. It's certainly an interesting time to be considering buying (or not buying) some of these.

Mobile devices – Blackberry are currently in the throes of a legal case which overshadows their entire business. Meanwhile Microsoft have released (but only just released) a new version of their mobile operating system which provides long absent security features. Mobile phones get yet more shiny and new functions added for Christmas.

Home networking – If you're more into home networking (which seems to be a new and somewhat curious subject of conversation down the pub) then there are plenty of choices here too.

USB data keys – Some companies give these away as publicity items. If you go to PC World or Currys you will see a forest of USB key drives right by the till (in the same way as Tesco put Mars Bars by their tills).

Security?

If you are tempted by these, don't overlook the security implications! Caveat Emptor (buyer beware) as regards mobile devices/smart phone security. These need to be regularly updated, just like your computer, to ensure that vulnerabilities found in the system are closed. You can even purchase a virus checker for smart phones and Windows Mobile devices. The number of smartphone viruses at time of writing is 94 (and growing). One virus has even been written to try and jump on to your PC from your mobile phone. Expect more of these!

Home networking, especially wireless networks, runs with the security off by default, so you need to turn it on. Look for a 'Wi-Fi' logo when you buy the device. Read up wireless security (see link below) and ask the seller awkward questions!

USB data keys, once lost, could be very embarrassing for you. Some types of USB key exist which provide security to prevent someone picking up the device in the street and copying the data. Many of these devices contain a password, but do not encrypt the data they contain, so the data may not be secure at all! Or you could encrypt the contents of the key by storing files within an encrypted container file on the key.

Out of site, out of mind?

Once offsite, many users have wireless network cards set up so they can download emails quickly from Starbucks or a myriad other wireless network points around the country. The world's largest Wi-Fi zone (94 acres) has recently opened at Canary Wharf. You can connect on a pay as you go basis. So you might think that it is OK to leave the wireless connection switched on.

However these devices also support small networks set up between two users. If a man on a train asked to plug a lead into your laptop from his laptop you would be unlikely to agree, yet with invisible wireless connections we think it is OK to leave them running, often without security, and inviting such connections!

Pervasive devices

Computing devices continue to get smaller and smaller. Perhaps you have been tempted by the new iPod Nano, the latest of Apple Computer's 'must have' music players. Moore's law (the one that says computing devices double in power every 18 months) has a corollary in that the size of existing devices with the same power can also be dramatically miniaturised. Sony's latest PS2 game console has the same capabilities as the previous version, yet fits on the palm of your hand. And you might have noticed (or bought) the playstation portable, an even smaller portable games console.

So where else are these devices going? One place that they are going is on to passports in the form of identifying RFID (radio frequency identity) tags which will contain at least some biometric data. Will the government be able to resist the temptation to put other data on these devices as well? It seems hard to resist, since the industry's overall trend seems to be to put all digital data into one place, judging by the convergence of camera, MP3 player, web browser and email onto the mobile phone. Another place in the longer term (when the project gets off the ground) is on to the government's proposed ID card scheme.

Perhaps I should restate the question. With the devices in place, the question becomes 'where am I going', since the technology provides the potential to correlate many trails of data we leave behind in everyday life. If you haven't read the Information Commissioner's comments on the ID card bill, do follow the link below. This raises some significant issues about the amount and nature of data in scope and the use to which it might be put.

Happy Holidays!

Links:

iPod Nano – http://www.apple.com/ipodnano/

Information Commissioner – http://www.informationcommissioner.gov.uk/cms/DocumentUploads/The_identity_cards_bill_ICO_concerns_October_2005.pdf

Wireless security – http://www.wi-fi.org

IRMA
Information Risk Management & Audit
40th ANNIVERSARY YEAR, 1965-2005
Happy Birthday

Chairman Alex Brewer cuts the cake to celebrate IRMA's 40th anniversary and uses the opportunity to practice for his next career move.

The Down Under Column

Bob Ashton – IRMA Oceania Correspondent

"Locked" Spreadsheets and Metadata Risks

Westpac, Australia's oldest bank was forced to request the Australian Stock Exchange to suspend its shares from trading early in November after its full year profit figures were inadvertently released to a number of analysts before the information was officially released to the market. The bank had sent by email a template containing its financial results to 37 analysts in 16 broking firms, before finalization and lodgment with the Australian Stock Exchange.

The template took the form of a spreadsheet, consisting of cells containing public information, and others containing secret data referring to the 2004/5 financial year's earnings. The latter had been pass word protected by Westpac in the belief that the contents would appear blanked out to the recipients. Unlocking pass word protected cells in an Excel spreadsheet is a trivial task, the instructions for which can be discovered with a few key strokes in Google. Two of the recipients unlocked the cells and informed Westpac of the disclosure.

Similar risks in regard to unintended exposure exist with documents containing metadata.

Meta data can be defined as data about data. Meta data describes how and when and by whom a particular set of data was collected, and how the data is formatted. - Webopedia.

Electronic documents can contain many types of information which is not immediately apparent to their users, including:

- Authorship
- Recipients
- email addresses
- Organization's name
- Name of computer, server and network on which the document resided
- Deleted text
- Hidden text

This data can be used to construct an audit trail of the history of the document.

Risks

In addition to privacy considerations, an example of the risks represented by metadata would be a law firm which recycles documents between several clients and finding their high fees difficult to justify if this became widely known. Other risks include:

- Confidential and sensitive information, which was believed to have been removed can be recovered.
- Names of authors, reviewers and company names can be revealed.
- If documents are recycled between clients sensitive information such as prices, terms and client's names can be disclosed.
- Internal network and file naming structures may be revealed.

Software affected

All the components of Microsoft Office, including Word, Excel and PowerPoint, Portable Document Format (pdf) files produced by Adobe Acrobat and Corel WordPerfect files can all contain metadata.

Safeguards

Organizations need to develop policies in regard to their tolerance of meta data in electronic documents. In most cases the safest option is not to allow any meta data attached to documents to be sent outside the organization.

Based on an assessment of risk, procedures need to be developed to address the issue in the following ways:

- The means by which meta data can be minimized in documents when the are first created and subsequently edited must be documented and promulgated to staff. The Microsoft Knowledge base contains detailed information on how this can be achieved.
- Manual procedures can be developed to remove meta data from sensitive documents.
- Software is available which can strip documents of metadata, and which can be set up to scan all documents which are emailed to an outside destination.

The Metadatarisk.org web site is a valuable resource providing information on this type of risk. Information is provided on the consequences of sharing certain types of information, the liability issues, and the risks to organizations in the mismanagement of metadata.

Threat-Based Security Engineering (TBSE)

John Leach

Abstract: TBSE is a risk modelling technique which models the dynamics of security interactions analytically making it possible to forecast risk in numerical form. It applies non-deterministic techniques to calculating the probability distribution of specific security outcomes as a direct function of the measured threat profile and countermeasure settings. Security engineers can design security solutions which provably meet QoP targets across a specified range of threat levels, and can optimise security settings to minimise cost or operational impact. Technical managers can perform precise cost/benefit analyses and can demonstrate compliance to policy or regulatory mandates objectively. TBSE can be applied to any threat (physical or logical, accidental or wilful, internal or external) and any security measure (technical or non-technical). This paper introduces TBSE and shows some of TBSE's early results. It briefly points to the potential impact of TBSE on the future practice of Information Security.

1 Introduction

Information Security has long been regarded as more an art than a science. We are all familiar with the problems this brings. Business management would like to perform cost/benefit analyses based on meaningful numerical values for protection and risk, and to be able to demonstrate to stakeholders that the organisation is compliant with internal and external mandates. Security practitioners would like to have clear and objective QoP targets set for the security solutions they are charged to provide, and then would like the ability to show whether the security solutions they design satisfy those targets within a specified threat range. None of these things can we do.

People understand from common sense and experience that security measures protect against threats, and they have an intuitive expectation that applying more security, whatever that might mean, should lead to the information assets being better protected, however that might be measured. However, looking beyond intuitive expectation, there are no ready techniques available for calculating the degree of protection provided by security measures and for quantifying the risks which result. Hence, people are left to build security solutions based on experience and on "best" or established practice. Each person is left to decide for themselves which security measures provide the most benefit and to judge what depth of defence is needed to achieve adequate protection.

2 The Form of Modelling Solution Needed

These inabilities and shortcomings arise because of the lack of any general techniques for describing or modelling the dynamics taking place between threats and security measures, the dynamics which lead to security breaches occurring. There is no general method with which to describe how any given security measure engages with the prevailing threats, how it modifies or counters the activity of those threats, and what the probabilities of the various possible outcomes might be as a result.

What form should a potential solution take? It would need to be a general purpose model with which one could describe the end-to-end risk process, i.e. the various processes or interactions by which security attacks are generated, those attacks engage with the target information asset, breaches do or do not occur, and how those breaches could lead to disruptions of the system and operational damage to the asset owner.

A general purpose model of this kind would allow the external inputs (e.g. the threats) to be described in a suitable form, descriptions created of how security measures are deployed, the effects of those measures on the parts of the risk process with which they engage to be quantified, and the arithmetic to be performed as needed to produce numerical results from the threat/security measure interactions.

The numerical results should be in a form from which the probabilities of particular specified outcomes occurring can be calculated. Outcome probabilities might be provided in the form of a single number, i.e. an overall probability value, or more usefully as a function of one or more relevant parameters, i.e. a probability distribution describing how the probability of the outcome varies as a function of relevant attributes of the threat and relevant parameters for the security measures applied.

Such a general purpose model would enable security risks to be measured and managed directly and reliably. One would measure the threats of interest and profile them according to relevant parameters. Using the model, outcome probabilities and appropriate risk indices would be calculated for any given security measure deployment. The security measure parameters within the model would be varied and the effects of those variations on the resulting risk indices calculated.

Information asset owners would set QoP targets for their assets, specifying the limits on outcome likelihood or impact they would be prepared to tolerate. Security engineers would determine the security measures and settings required to satisfy those QoP targets given an expected level of threat. They would calculate how the risk indices would vary across a range of likely threat profiles, and how the countermeasure settings should be adjusted for those QoP targets to remain being satisfied. Once security measures had been deployed, regular measurement of the actual threat profiles to which the information assets were exposed would allow security settings to be adjusted as needed for the information assets to remain continuously protected to the asset owner's satisfaction.

Reaching this goal would be a landmark achievement, enabling security to be deployed with confidence and its benefits to be understood in business terminology. Spending decisions could be made based on reliable data, and security measures implemented to provide a specified level of protection according to business need and budget.

3 TBSE and Some Examples of its Results

The requirement, then, is for a methodology and techniques with which to model the end-to-end dynamics between threats and security measures, the dynamics through which security outcomes and risk are created. There may well be several possible routes by which to achieve this. This paper will describe one approach, TBSE, which is just such a modelling technique and which has been able to achieve the type of results described above using real-life threat data. This paper will describe some of these results, and then describe TBSE in outline and indicate its potential.

TBSE is a general purpose technique for modelling security interactions analytically and calculating outcome probabilities in numerical form. It employs non-deterministic modelling techniques for solving security risk problems. It can be applied to any threat and any security measure, and can model multiple threats and multiple countermeasures working in parallel.

In principle, TBSE can be used to build customised risk models which describe corporate information infrastructures and to calculate a wide variety of risk indices for the many threats and many security measures all working in parallel. In practice, it would be a complex exercise to build such sophisticated models in one step. For this reason, TBSE has, in the first instance, been applied to a number of simpler problems. Three such risk problems and their results will be described in this paper.

3.1 E-mail Viruses and Anti-Virus Software

The first real-life problem to which TBSE has been applied is that of quantifying a user's risk of e-mail virus infection as a function of the way their anti-virus (AV) software is deployed. This has been a collaborative project undertaken with MessageLabs (http://www.messagelabs.com). The results will be freely available in due course on the MessageLabs' web site.

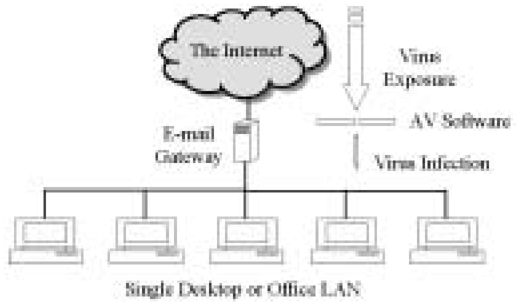


Fig. 1. The Scenario Modelled with MessageLabs

Visitors to the web site will be able to use the MessageLabs "Risk Calculator" to calculate the probability of an infected e-mail making it past their AV software as a function of how that software is deployed. Results are provided in a variety of numerical forms to ensure their accessibility for the untrained user. The visitor will be able to determine their risk and exactly how that risk would vary if they were to change their AV settings. As a result, they will be able to work out accurately how to configure their AV defences to cut their risk by a half, by three quarters, by whatever level they choose.

The scenario modelled in this work is shown in Figure 1. The threat from e-mail viruses is carried to the target (e.g. an office LAN) by e-mails arriving at the e-mail gateway. Even though the gateway hosts some Anti-Virus (AV) software, there is always a small risk that one or other virus will get through to the target. TBSE is used to calculate that risk in objective numerical form as a function of the measured threat and the way the AV software is configured.

MessageLabs starts by measuring the threat and displaying that in the form of a real-time chart, as in Figure 2 below. The threat, the flux of e-mail viruses arriving at the target, is profiled as a function of its relevant attribute, the age of the virus (in hours) at the time the virus is received at the e-mail gateway.

The visitor is invited to enter a few simple details which describe the volume of e-mails they receive on a typical day and how often they check for new virus signatures. TBSE then calculates the probability of an e-mail virus getting past their AV software in those circumstances.

The probability is given as an actual number, not in the common form of a High / Medium / Low estimate. Rather than showing the raw probability result, which would be a figure such as "one in 357,200 e-mails will carry a virus past your AV software given the description you have just provided", a result the untrained user might be unclear how to use, the risk result is provided in three alternative numerical forms, with the primary form being the probability (to the nearest whole percentage point) the user would have gone three months without any infected e-mails making it past their AV software based on the measured threat profile. Hence, the user gets a meaningful result they can understand straight away and can work with.

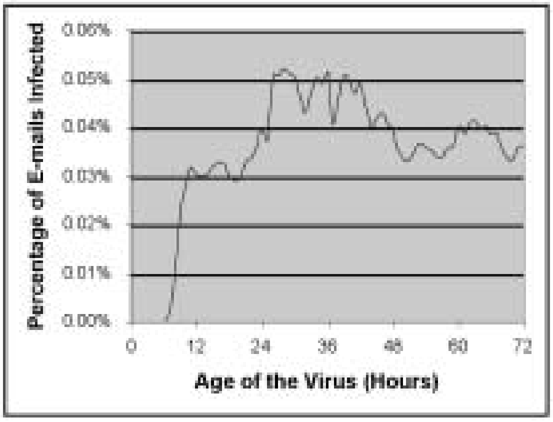


Fig. 2. The E-mail virus threat profile

The visitor is then given the opportunity to enter a different value for how often they check for new virus signatures. This lets them see exactly how their risk would fall if they were to strengthen their AV defence in that way. They can continue increasing their signature checking frequency until their risk is pushed down to a level they are comfortable with, at which point they will know exactly how often they need to be checking for new signatures if they are to achieve their desired level of protection. In practice, the visitor will have chosen a QoP target which expresses their tolerance for e-mail virus risk, and will have determined exactly how their AV protection needs to be configured to satisfy that target.

This project with MessageLabs shows how TBSE can be used to help people control their security risk in a direct and simple manner. It gives them an objective numerical figure for a particular risk, and allows them to adjust their risk to their chosen level by adjusting their countermeasure configuration in a specified way.

3.2 Worms and Software Patching

This second example uses TBSE to assess the benefits of software patching. It shows how one's probability of suffering a successful worm intrusion falls as the average time taken to apply a security patch is brought down, based on the measured profile of the worm threat.

The scenario being modelled is broadly similar to that shown for the preceding example except that the threat in this instance is the threat from worms coming in over the target infrastructure's Internet connections. Whereas the first example showed TBSE modelling a security defence which blocks attacks, this example models a security defence which reduces the target's susceptibility to the threat. It would be a simple extension to combine the two models to show the combined effect of the two different types of security measure working in tandem, a problem of obvious interest to every large Internet-connected organisation.

The work behind this example calculated a target's risk of a successful worm attack, for worms which exploit one (or sometimes more) Microsoft software vulnerabilities including, in particular, the LSASS vulnerability. The LSASS vulnerability was very popular with worm writers. The results for the LSASS vulnerability were compared with those for the average of ten other worm-exploitable vulnerabilities each of which was less actively used by worm writers.

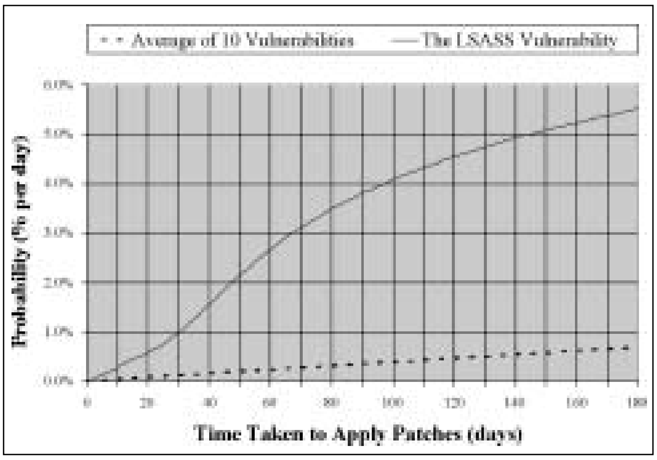


Fig. 3. The probability of a successful worm attack

Figure 3 shows the risk of a system suffering a successful worm attack as a function of the rate at which patches are applied (based on real-life threat data). This shows how the risk rises for an average-risk vulnerability as it waits to be patched, and how much faster the risk rose for the LSASS vulnerability. The modelling presumed a patch management process whereby all vulnerabilities are patched according to a regular cycle; after a certain time period the system manager rolls up all the patches released since the previous round and applies them all at the same time after an allowance for testing.

For average-risk worm-exploitable vulnerabilities, the IT system manager on a 90-day patching cycle has a probability of suffering a successful worm attack due to an unpatched vulnerability (discounting any other countermeasures they might have in place) of 0.35% per day per exposed IP address. If they were to move to a 30-day patching cycle, their risk would drop to 0.15% . A sample of these results is given in Table 1 below.

Table 1. *The probability of a worm successfully exploiting an average-risk software vulnerability for a range of patching cycle lengths*

Patching cycle (days)	Probability per day	Probability per month	Probability per quarter	Probability per year
30	0.15%	4.0%	10%	35%
60	0.25%	7.0%	20%	60%
90	0.35%	10%	25%	75%

For a high-risk, i.e. an actively exploited, vulnerability such as the LSASS vulnerability, the risk is, naturally, much higher. The comparable results for the LSASS vulnerability are shown in Table 2.

Table 2. *The probability of a worm successfully exploiting the LSASS vulnerability for a range of patching cycle lengths*

Patching cycle (days)	Probability per day	Probability per month	Probability per quarter	Probability per year
30	1%	30%	70%	99%
60	3%	60%	93%	100%
90	4%	70%	97%	100%

Hence, if IT system managers do not have a way to identify which vulnerabilities are high risk, then even if they put in the effort to patch their system regularly on a 30-day cycle, they are still placing themselves at considerable risk.

The above scenario was modelled on the basis of the system manager not having a way to identify high-risk vulnerabilities. Of course, many organisations do get advised by their vendors or suppliers in advance whenever a new high-risk vulnerability is about to be publicised. In these situations, IT system managers are able to patch high-risk vulnerabilities on an accelerated patch management path. TBSE has been used to model this variation in the scenario to show by how much adopting a more flexible patch management approach reduces the risks.

Assuming users identify high-risk vulnerabilities and then patch those with only a short delay for testing, the results are as shown in Table 3.

Table 3. *The probability of infection by a high-risk vulnerability for a range of patching delays*

Time taken to install the high-risk patch (days)	1	2	3	4	5	6	7	10	14	21
Probability of being infected before the patch goes in (%)	1.8	3.6	5.3	7	8.5	10	11.5	15	20	32

These results show clearly the need for high-risk vulnerabilities to be identified and patched as soon as possible, and provide IT system managers with a guide to just how quickly they should aim to have high-risk vulnerabilities patched. These results allow the system manager to explore various options for how they might meet the system owner's QoP target for the system, and to ensure that they have not only adequate resources but also adequate flexibility if they are to adopt a twin-track strategy for patch management.

3.3 Unauthorised Behaviour by Staff

The examples above show TBSE being used to model technical countermeasures and technical threats. TBSE has also been used to model the interactions between non-technical countermeasures and the threat of staff knowingly violating a (written or unwritten) code of authorised behaviour. This threat is a broad one including, at the low-severity end of the spectrum, activity such as the unauthorised use of corporate IT facilities for personal purposes and, at the high-severity end, significant financial fraud. TBSE can be used to assess the effectiveness of different countermeasures at reducing the rate or severity of staff attacks, and can help the security manager select countermeasures to achieve specific effects.

Three countermeasures were analysed to assess their effects on reducing the rate and/or severity of attacks arising from staff misbehaviour. The three were: strengthening the security culture; security vetting; increasing deterrence. The results showed that:

- Strengthening the organisation's security culture reduced the rate of attacks more than it reduced the severity of attacks;
- Security vetting reduced the rate of attacks and the severity of attacks in broadly equal measure;

- Increasing the accuracy of security vetting beyond a moderate level requires more effort by the vetting organisation and is, perhaps, fairer on staff but appears to give almost no benefit in terms of the end results achieved;
- Increased deterrence had a strong effect reducing the rate of attacks but only a small effect reducing the severity of attacks.

Conclusions: Security vetting is very helpful, but only up to a point. Deterrence reduces the risk only to the degree that it reduces the expected rate of attacks. Strengthening the security culture is the way to achieve the greatest risk reduction if an organisation plans to deploy only a single one of these three countermeasures. The most cost-effective risk reduction comes from deploying a mixture of these countermeasures with the main reliance being placed on security vetting and building a strong security culture.

These are signal results, never before achieved, and show how valuable risk modelling can be even in the absence of precise data.

The results from this third TBSE example were, in the absence of real data, based upon a number of hypotheses regarding the threat profile of staff and how staff modify their behaviour in response to the three different countermeasures. These hypotheses are believed to be sound and to provide a strong basis for the analysis performed. However, it is clear the above results should be treated as indicative, not definitive, until the assumptions on which they are based have been validated.

Those assumptions are eminently testable. By measuring the relevant characteristics of the threat population and by calibrating the way these personnel countermeasures work, TBSE analyses can be conducted using data representative of real situations. The results achieved would then be definitive results of highly significant value.

4 TBSE in Outline

The above examples show that TBSE has the power to address a variety of different scenarios and a variety of different modelling needs. The results can be used to develop numeric QoP targets for specific outcomes or for broad classes of outcome, and can be used to show the level of protection provided by a single security solution or several security measures working together.

TBSE is a fully general model applicable to all types of threat and all types of countermeasure. In the remainder of this paper, we will describe TBSE in outline and indicate how it could support new Information Security services and products.

TBSE is based around a model which allows us to create suitable analytic expressions for the various interacting components and which leads to tractable measurements and calculations. The model describes the creation of security incidents and the resultant impact of those incidents as a series of dynamic processes. This is shown schematically in Figure 4 below.

In the model, a population of Threat Agents generate a population of attacks. That population of attacks creates a population of security breaches, which themselves give rise to a population of system disruptions which lead to a population of damages. Each population is described in terms of a number distribution in relevant attributes. The processes by which one population engenders the next population in the chain can be described by appropriate analytic functions.

The ways in which countermeasures affect the dynamics of the processes in the chain are themselves described by suitable analytic functions. Different countermeasures work at different points of the chain.

- Some work to reduce the population of attacks generated by a population of threat agents. Examples include security vetting, security culture and deterrence, all of which work to reduce the population of attacks generated by misbehaving staff.
- Some countermeasures work to reduce the population of security breaches created by a population of attacks. Examples include firewalls, anti-virus software and software patching.

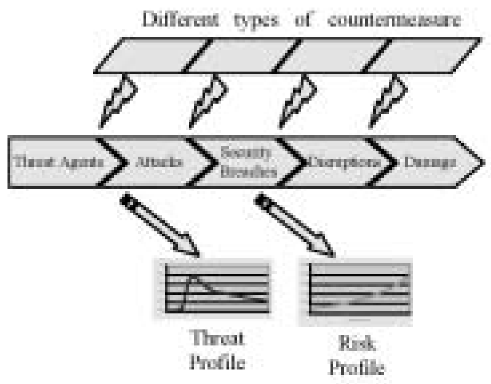


Fig. 4. TBSE Schematic

- Some countermeasures work to reduce the population of disruptions caused by a population of security breaches. Examples include intrusion detection and having a warm standby server. Intrusion detection doesn't stop an intrusion but makes it more likely action can be taken to reduce the severity of any disruptions caused. A warm standby server doesn't stop the main server having an outage but reduces the severity of the disruptions caused each time an outage occurs.
- Some countermeasures work to reduce the damage a population of disruptions leads to. Examples include having contingency arrangements for disrupted business processes, and insurance. Neither reduces the rate or severity of the disruptions which occur but each can reduce the degree of damage (whether measured financially or otherwise) those disruptions might cause.

TBSE can be used to model one link in the chain or several links in the chain, and to model one or more countermeasures operating within the chain. For each of the first two examples above, the threat (the flux of attacks reaching the target system) was measured and TBSE was used to model how the respective countermeasures influenced the likelihood of those attacks creating security breaches. In each example, just one link in the chain was analysed, and just one countermeasure in each link. We did not analyse how other anti-virus measures, e.g., training staff not to open suspicious attachments, or how other anti-worm measures, e.g., a firewall, might further reduce the population of security breaches caused. Each example could easily have been extended to cover additional countermeasures.

We also did not need to start from the top of the chain each time. Lacking information describing the population of virus or worm writers and any description of the rate at which those writers create viruses and worms, we simply measured the populations of attacks experienced. By hypothesising the rate at which those populations create viruses and worms, we could, if we wished, use TBSE to deduce the populations of threat agents needed to generate the profiles of threats observed. Alternatively, if we could measure the populations of threat agents, we could understand the rate at which writers write viruses and worms by deducing the functions needed to create the measured threat profile from the measured threat agent population.

Thus TBSE allows us to model either just one stage of a particular threat chain or to model the whole chain, and to calculate either upstream or downstream components in the chain depending on our purpose and on which components we can describe or measure.

TBSE does not require the data upon which it works to be of the highest quality; it will work with precise or imprecise data as available. Clearly, the more precise the measurements of the input populations, or the more precisely an analytic function can be formulated, the more accurate the results should be. Some threats can be measured accurately with ease, others less so. Hence, results will be of greater or lesser precision accordingly. However, given the inability of today's non-analytic methods to produce results with any accuracy, even results which are accurate to only ± 50% would represent a significant improvement on the results otherwise available today.

5 E-mail viruses and AV software (Revisited)

Equipped with this initial understanding of TBSE, we shall revisit the first example described above and look more closely at how the results were generated.

Anti-virus software was modelled on the basis that it scans all incoming e-mails looking for any instances of a known virus signature[1]. The user's AV vendor continually releases signatures for new viruses as new viruses are reported, and the list of reference signatures held on the e-mail gateway is updated by the user periodically, sweeping up all the signatures released by the vendor since their previous update. The release of signatures by the vendor and the periodic update of signatures by the user are asynchronous; the user checks for new signatures with a given regularity irrespective of whether their vendor has released none, one or many new signatures in that period.

The probability of the user's AV software detecting a virus in an e-mail is presumed to be 100% provided that virus' signature is held in the software's local signature store. The probability of a virus being detected by the AV software at the moment the target is exposed to that virus then depends on the age of the virus at the time the system is exposed to it and whether, by that time, the vendor has released the relevant signature AND the user has picked up that signature through their signature update process.

If a user is exposed to a new virus before the vendor has released the signature, the probability of the virus getting past the user's AV software is assumed to be 100%. If the user is not exposed to a new virus until well after the vendor has released a signature for it and the user has had time to update their reference store, the probability of the virus getting past the user's AV software is taken to be 0%. In the intervening period, the probability is somewhere between 100% and 0%.

That probability curve can be calculated accurately and, clearly, it will be a function of the frequency with which the user checks for signature updates. The more frequently the user checks for updates, the more quickly the probability curve will rise from 0% to 100% with increasing age of the virus.

In the work performed with MessageLabs, we collected a large amount of data describing how quickly vendors released signatures after a virus was first detected. The data covered nearly twenty vendors and over thirty virus strains. From this data, we constructed a curve showing the probability of the AV vendor having released a signature as a function of the age of the virus, with the results being weighted according to vendor market penetration. This was combined with the frequency the user checks for new signatures to give the probability of the user having a virus' signature in their local reference store at the moment they are exposed to a virus, for any virus, as a function of two parameters, the age of the virus at the moment of exposure and the frequency with which the user checks for signature updates.

Interestingly, the results showed that, for a user exposed to a new virus before their vendor has released a specific signature for it, the probability of the virus getting past the user's AV software is NOT actually 100%. There is a probability of about 10% that one of the reference signatures already in the local signature file will be sufficient to catch the new virus. Whether or not a new virus is caught by an old signature varies from vendor to vendor, as different vendors build signatures in different ways depending on their differing methods and analysis of how each new virus works.

The probability of the user having a virus of a given age slip past their AV software is then the probability of the user being exposed to a virus of that given age and the probability that, when they are so exposed, their AV software will not have that virus' signature in its local signature list. The latter probability is obtained directly from the probability distribution we have just described. The former, the probability of exposure, is obtained by measurement of the threat.

MessageLabs counts, from the millions of e-mails it manages each hour, the number of e-mails carrying a virus of a given age, for all ages from zero hours upwards. It performs that measurement afresh each hour, each day, to create the threat profile as shown in Figure 2. That profile is combined with the probability distribution described earlier to calculate the probability, per e-mail received by the user, that the e-mail will carry a virus for which the user does not yet have a suitable signature in their local signature file. This is the probability of the user having an infected e-mail slip past their AV software, and it is a direct function of how often the user checks for new virus signatures.

All the user has to do to determine their risk is say how many e-mails they receive in a typical day and how frequently they check for new signatures. TBSE works out their probability of infection based on those two values and the current threat profile.

6 Conclusion

For many years, the Information Security industry has struggled to develop a way to model the interactions which lead to Information Security risk and to forecast security outcomes in an objective analytical manner. Our inability to achieve this goal has clearly hampered the advance of Information Security as a discipline.

TBSE shows how proven non-deterministic modelling techniques can be applied to the forecasting of security risk. Though it has been suggested in the past that non-deterministic techniques might offer a solution to this modelling problem, we believe that TBSE represents the first time it has been shown in full how such techniques might be applied and the types of results which can be generated. It transpires that this type of modelling is simpler than many people had anticipat-

[1] The model used in our example contained no heuristic scanning component. This does not mean that TBSE has difficulty modelling heuristic scanning, just that heuristics were not included within this example. AV software which performs both signature-based and heuristic scanning could easily have been modelled with a simple extension of the model.

ed and is much simpler and more accurate than relying on huge data mining engines extracting imprecise correlations from terabytes of raw data. This is extremely exciting and opens the prospect for major advances in the security field.

TBSE is of direct benefit to user organisations seeking to improve the effectiveness and efficiency of their security risk management arrangements.

- Users will be able to specify QoP targets for information systems in the form of the maximum levels they will tolerate of threat or outcome populations.
- Security solutions will be designed which can provably satisfy specified QoP targets for a given range of threats, and security evaluations of vendor products will become objective rather than purely relative.
- Dashboards will be created allowing top management to exercise strategic rather than tactical oversight of the organisation's risk management arrangements.
- Threats would be measured continually so that security parameters can be adjusted to ensure QoP targets continue to be met against the changing threat.
- A broad range of metrics will be deployed so that security solutions can be compared objectively against their claims and the effectiveness of locally deployed security practices compared meaningfully across disparate teams and circumstances.

TBSE also creates a wide variety of commercial opportunities for service providers and vendors wishing to support this global user community. Managed services companies can build new services to supply their customers with threat data and the algorithms to turn monthly threat indices into forecast risk indices. Management consultancies can build new services to help their clients tailor risk models and decision-support tools to match their client's particular environments. Security assurance companies can develop services to calibrate security countermeasures and to certify the effectiveness of security deployments. They will address the need for a new range of compliance audits to enable:

- Companies to assure audit committees they have a security programme in place which protects shareholder interests and information assets;
- Companies to demonstrate objectively and measurably to external regulators that they are operating in compliance with regulations and legislation;
- Business partners to be assessed to ensure they do not introduce inappropriate risks to the integrated supply chain.

TBSE will create opportunities for product companies to develop new risk management software tools. TBSE might also be what is needed to kick start an active Digital Risk insurance marketplace by enabling the development of simple Digital Risk insurance products for which premiums can be reliably priced.

Dr John Leach has been an Information Security consultant for nearly 20 years, for the past three of which he has been an independent. His doctorate included modelling physical processes using the type of modelling techniques which are now being used in a much simplified form to underpin TBSE. He may be contacted on +44 1264 332 477 or by e-mailing john.leach@jlis.co.uk

Letter to the Editor

Dear John,

I read your nostalgic Editorial in the first issue of this season's I.R.M.A. Journal with interest, and felt that for the record I might add a few things. The group started out in about 1963 as an informal discussion group. Eric Hinchcliffe, who was then the auditor to the Coal Board joined up with Miller Ross of Peat Marwick Mitchell (now KPMG) to get some discussion going on the audit problems around computer systems. A few meetings were laid on at the basement rooms of Hobart House, Grosvenor Place (HQ of the N.C.B.) and in fact I lectured at the second or third of these on 'Computer Fraud', having been invited to join the group. Eric became Chairman and Miller acted as Secretary. As the meetings evoked sufficient interest and were seen as successful, then it was decided to apply to the BCS to become a group under their umbrella. Negotiations to become a Specialist Group were a bit involved and were handled by Eric and Miller with Cecil Marks (Head of the Civil Service College in Victoria) representing the BCS.

At the time, the BCS did not show much interest in business application, being mainly concerned with the computer as a machine and with programming skills (thank goodness they gradually changed their viewpoint). Computer auditing was not then acceptable to them and ultimately the title 'Auditing by Computer' was devised. Fortunately, the first packages such 'Find 1' (which was too complex for general use) had just been made available and 'Find 2' was about to come into wider use (hence DART and EARS), and this development gave a platform on which to let us in. It was not to be until Willie Lists's time as Chairman that Computer Audit became acceptable. After a few years, Eric left the Coal Board to go to Hambro's Bank and we lost our meeting centre at Hobart House. After a short while at Puddle Dock, meeting places became seasonal at such places as Regent Street Polytechnic, Connaught Rooms, Overseas Club and Charing Cross Hotel.

My computing experience goes back to the mid 1950's when I went on courses at Northampton Polytechnic (now City University) and ICT at Cookham. At the same time, we were investigating the use of Elliott valve machines (405) for use in the office and did quite a lot of systems analysis work on wages (the worst subject we could have picked), but when the valves blew several times on demonstrations, it was decided to wait for something more reliable. Soon the silicon chip arrived and we got machines like IBM 1100, ICL 1301, Elliott 803 Honeywell, and NCR 315 with its magnetic card strip storage. Then operating systems became developed, giving greater ease of use and appearing in IBM 360 and ICL 1900 series. I became deeply involved in the development of the use of the Elliott/NCR 4100 at Kingston Polytechnic, to which I had then moved. It was then that I started programming in assembler and machine code (patches could be done in machine code). At the same time, I was working in Basic and Algol and later took on Filetab. Nowadays, I do not have any contact with computer systems and am way out of date on such matters.

I note that the Journal is to go 'online' in the near future. I shall miss it as a contact with the past as I have no access, but all good things must come to an end. I still have all issues except the first (which I gave back to Ginny Bryant, who was then editor and did not have a copy for herself).

With best wishes.

Fred Thomas
(IRMA Treasurer Emeritus) Great Dunmow,Essex

What is Effective Project Risk Management?

Sofia Rashid and George Allan – University of Portsmouth, UK

Introduction

There are always risks associated with a project; therefore it is important to take measures to reduce these risks using risk management techniques. Risk management should be considered as a major topic within project management; if risks are not dealt with properly they may cause a project to fail. The purpose of risk management is to ensure that levels of risk and uncertainty are properly managed so that the project is successfully completed (Government of Tasmania, 1995). This paper will discuss what risk is, how it is managed effectively and how risk management documentation is presented.

What is Risk?

The term risk is associated with many human endeavours, be it nuclear reactor construction, company acquisition, or information systems development (Barkki 1993 p. 204). In the literature on risk management/control many authors have attempted to define risk. Lowrence describes risk as a measure of the probability and severity of adverse effects (Haimes 1992 pp5, 53). Rowe explains risk as the potential for unwanted negative consequences of an event or activity (Ansell et al 1992, p 4). Rescher defines risk as the chancing of a negative outcome. He goes on to say that in order to measure risk we must accordingly measure its defining components, the chance and the negativity (Ansell et al 1992, p. 5). Knight describes risk as the form of incomplete knowledge where the future can be predicted through the laws of chance (Pender, 2001, p81).

McNamee 1997 suggests risk is a concept that describes uncertainty in achieving goals; he further goes on to say that risk is never managed, as risk is a theoretical property. What most risk definitions have in common is that risk has some aspect of uncertainty and loss. Uncertainty can be defined as the variability of the future outcomes, where probability can be predicted (Pender, 2001, p 81). Therefore a good definition of risk is the uncertainty about a situation; that is the possibility of loss, damage, or any undesirable event. It can therefore be seen that risk and uncertainty are concerned with incomplete knowledge over future 'states of nature` (Pender, 2001, p82).

Many projects desire low risk, which would mean a high probability of a successful outcome in terms of profits, quality and time (Decisioneering, Inc 2001). Practicing managers have known that managing uncertainty is important and as a result many companies have established risk management departments to control the risks that they might be exposed to (Akintoye and MacLeod, 2001, p31).

What is Risk Management?

Risk Management is a practice in which one can identify and mitigate risks in a project. It involves a well-organized environment for hands-on decision making to (Carnegie Mellon University 2001): -

- Assess risks continuously throughout a project.
- Determine and prioritise those risks that may have a considerable impact.
- Implement strategies to deal with the risks identified.

By no means should risk management be seen as a one-off activity: risks should be monitored throughout the project as threats can emerge or their impact or likelihood change. Government of Tasmania (2001) suggest that risks should be assessed roughly every two weeks.

Many people may have the misconception that once risk management is done, the project will be a success. However, there are many aspects to achieving project success. Risk management is not a silver bullet (Carnegie Mellon University 2001) but risk management can improve decision making, help avoid surprises and increase chances of success.

McNamee believes that risk management is a misleading phrase. He states that risk is never managed, since risk is a theoretical property. It is the organization that is managed in expectation of uncertainty (which is characterised by risk) (McNamee, 1997).

Risk management consists of two broad categories: Risk Assessment and Risk Control.

- Risk Assessment - Identifies and analyses risks
- Risk Control - Takes steps to reduce risk and monitor improvements

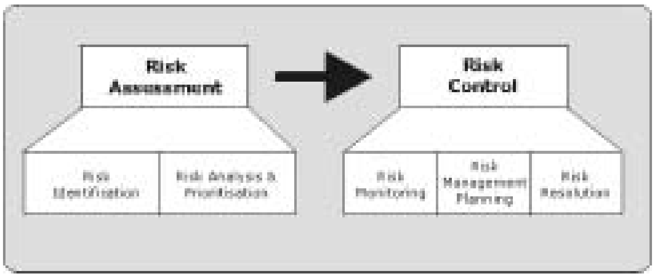


Figure 1. *Illustration showing the elements and relationship between risk assessment and risk control.*

Risk Assessment

This paper sees risk assessment as an important feature of risk management, because without risk assessment, risk control cannot begin. Risk Assessment can take place at any time during the project, although the sooner the better. It is important that risk management identifies and manages risks on a regular basis throughout the entire life cycle of the project.

Kaplan and Garrick believe that risk assessment is the job of the analyst, who tries to answer the following questions (Haimes, 1991, p. 20):

1. What can go wrong?

2. What is the likelihood of it going wrong?
3. What are the possible consequences?

Risk assessment comprises two main sub categories:

1. Risk identification,
2. Risk analysis and prioritisation.
3. Risk Identification

This stage identifies and defines any risks that may have a negative effect on the success of the project (Holt, 2001). There are many ways to identify risk, including; using past experiences and lessons learnt from previous knowledge, researching into relevant issues for the project, looking at checklists (an example is Boehm (1991) who identifies the ten most important risk items, and builds on them), and finally the use of questionnaires, which should be periodically reviewed.

A good means for identifying risks is using checklists. Boehm (1991, p35) suggests that risk identification checklists should be developed as a guide to the process. He then goes on to develop a table (based on information provided by experienced project managers) that recognises the main sources of risk and possible management techniques to resolve or avoid those risks.

1. **Personnel Shortfalls:** Staffing with top talent; job matching; team building; morale-building; cross-training; prescheduling key people.
2. **Unrealistic Schedules and Budgets:** Detailed, multisource cost and schedule estimation; design to cost; incremental development; software reuse; requirements scrubbing.
3. **Developing the wrong software functions:** Organizational analysis; mission analysis; operational concept formulation; user surveys; prototyping; early users' manuals.
4. **Developing the wrong user interface:** Prototyping; scenarios; task analysis.
5. **Gold-plating. Requirements scrubbing:** prototyping; cost-benefit analysis; design to cost.
6. **Continuing stream of requirements changes:** High change threshold; information hiding; incremental development (defer changes to later increments).
7. **Shortfalls in externally performed tasks:** Reference-checking; pre-award audits; award-fee contracts; competitive design or prototyping; team building.
8. **Shortfalls in externally furnished components:** Benchmarking; inspections; reference checking; compatibility analysis.
9. **Real-time performance shortfalls:** Simulation; benchmarking; modeling; prototyping; instrumentation; tuning.
10. **Straining computer science capabilities:** Technical analysis; cost-benefit analysis; prototyping; reference checking.

Table. 2. *Boehm's ten most important software risk items (adapted from Pfleeger 2001).*

Risk Analysis and Prioritisation

Once the risks have been identified, they are then evaluated to assess the potential impact on the project. The risks are individually assessed in three ways:

1. Firstly, the likelihood of the risk occurring.
2. Secondly, the consequences faced by the project if the event occurred.
3. Thirdly, prioritising the risks that will have the most impact on the project.

Once the risks have been identified the risks need to be analysed/prioritised. This is done by assessing the impact and probability of the risk actually occurring (Holt 2001). Risk prioritisation can be done by various methods including scenario analysis, decision trees and risk matrix.

Scenario Analysis – a number of probabilities and the likely outcomes are investigated for a wide range of scenarios, which lead to the production of a decision-making matrix. From the matrix a number of varied combinations can be chosen, as it provides numerous choices.

Decision Trees – are risk models in which the percentages of success and failure of a number of solutions can be obtained, so that the financial outcome can be determined.

The most commonly used method is risk matrix; this is a tool, which can be used to prioritise risks that may have an impact on the project. The risk matrix provides a structured method for prioritising risks. Threats are graded according to the likelihood they will be realised and the impact they will have if they do occur (Government of Tasmania 1998). Potential threats can be classified according to whether there is a low, medium or high likelihood that the risk will occur and whether their impact will be low, medium or high.

Table 3 illustrates a risk management matrix table assessing the likelihood and impact of potential threats to a project. This will give a good indication of the risks that the project may face.

Threat	Likelihood			Impact		
	Low	Med.	High	Low	Med.	High
Inadequate funding		X		X		
Lack of technical skills			X			X

Table 3: *Risk matrix table (adapted from Government of Tasmania 1998)*

As mentioned before, risk rating is often described as being Low, Moderate, or High. This is based on the following criteria:

Low Risk: Has little or no potential for increase in cost, disruption of schedule, or degradation of performance. Actions within the scope of the project and management alertness should result in controlling acceptable risk.

Moderate Risk: May cause some increased costs, disruption of schedule, or degradation of performance. Therefore in order to control acceptable risk, special action and management attention may be necessary.

High Risk: Likely to cause significant increases in cost, disruption of schedule, or a breakdown in performance. In order to control this type of risk, a high level of attention and action would be required by the management.

Once this process has been completed, the risks identified will allow the project manager to realise the most significant risks within a project and target them. By employing these various risk ratings methods, project managers can identify threats that require immediate action or that can be ignored. Thus, risk rating is seen as a fundamental part of risk analysis.

Risk Control

Risk control monitors and manages the risk in a manner that reduces the probability/likelihood and/or consequence/impact of the risk on the project. Risk control contains the following sub categories:

1. Risk management planning;
2. Risk resolution;
3. Risk monitoring.

Risk Management Planning

Following the identification of items that are seen as major risks to the project, a set of risk control plans need to be established by the company in order to keep the risks under control. Techniques such as quality monitoring, cost – schedule estimates, prototyping, and benchmarking are employed. Once the plans are organised, the second set of questions are addressed:

1. What can be done?
2. What options are available?
3. What are their associated trade offs, in terms of cost, benefits and risks? (Haimes, (1992), p. 20; Boehm. (1991), p. 38; Hall (1998)).

Risk Resolution

When risk has been identified and plans have been developed to mitigate it, it is important to take steps to implement the plans, to reduce the risk.

Risk Monitoring

At this final stage, risk monitoring involves systematically tracking and evaluating the effectiveness of risk handling actions. Monitoring is not regarded as a problem solving technique, but rather a proactive procedure that observes the results of how to handle and identify new forthcoming risks that may be involved. As new uncertainties are identified, the risks must be continuously monitored. This will include tracking those uncertainties that have already been mitigated: they may still have some underlying risks which will develop further on in the project life cycle.

Carnegie Mellon University (2001) believes that there are seven principles which provide a framework to accomplish effective risk management. These can been seen in table 4.

Global perspective	● Viewing software development within the context of the larger systems-level definition, design, and development. ● Recognizing both the potential value of opportunity and the potential impact of adverse effects.
Forward-looking view	● Thinking toward tomorrow, identifying uncertainties, anticipating potential outcomes. ● Managing project resources and activities while anticipating uncertainties.
Open communication	● Encouraging free-flowing information at and between all project levels. ● Enabling formal, informal, and impromptu communication. ● Using processes that value the individual voice (bringing unique knowledge and insight to identifying and managing risk).
Integrated management	● Making risk management an integral and vital part of project management. ● Adapting risk management methods and tools to a project's infrastructure and culture.
Continuous process	● Sustaining constant vigilance. ● Identifying and managing risks routinely through all phases of the project's life cycle.
Shared product vision	● Mutual product vision based on common purpose, shared ownership, and collective communication. ● Focusing on results.
Teamwork	● Working cooperatively to achieve common goal. ● Pooling talents, skills, and knowledge.

Table 4: *The seven principles which provide the framework for effective risk management*

Who is Responsible for Project Risk Management?

Many people within a project will have some responsibility for controlling the risks that are identified. The project manager, for example, is responsible for monitoring and managing all parts of the risk management process which would include:

- ensuring the progression and effectiveness of the risk management plan;
- identifying any new or increasing risks, by means of continually monitoring the project throughout its lifecycle;
- continually keeping the project sponsor and steering committee up to date with regular reports.

Though the project manager maintains constant responsibility, he may choose to hand over the project risks to a separate risk manager.

Other members of the team can also be of assistance with regard to the identification, analysis and assessment of risks, as well as assisting the development of the risk management plan. They can be seen as being responsible for risk mitigation actions.

Project stakeholders, reference groups, external consultants and more specifically the business owners may also be able to contribute by providing input into the risk management plan and being responsible for risk mitigation actions. The steering committee, whose prime responsibility is for the management of risks associated with the project, oversees the management plan and its periodic review. It is important to remember that risk management cannot entirely be the responsibility of one person and that it is a communal activity involving a range of people associated with the project (government of Tasmania 1988)

What Effective Project Risk Management Involves

- Commitment to risk management by stakeholders, corporate management, the project steering committee, the project manager and project team members.
- The project manager should take responsibility to ensure that both the project team members and managers have an understanding of the technical and non-technical issues related to the project.
- Risk management needs to be carried out throughout the lifecycle of a project, this ensures that the risks are continuously being monitored and assessed.
- Communication is essential by all members involved in the project.

(Government of Tasmania 1988)

Risk Documentation

There are several reasons why documentation is part of the criteria for successful risk management:

- It provides a basis for monitoring risk handling actions and verifying the results.
- It is a formality that tends to ensure more comprehensive risk assessment than if the process is not documented.
- It provides program rationale for program decisions.

A risk management plan is a tool which is used to outline all the possible threats identified before and during the project. It documents mitigating strategies, which are pursued in response to the threats identified. The plan should include (Government of Tasmania 1998):

- A description of each risk;
- An assessment of the likelihood it will occur and the possible impact if it does occur (low, medium, high);
- Grading of each risk according to a risk assessment table;
- Who is responsible for managing the risk;
- An outline of a proposed countermeasure;
- Estimated cost for each countermeasure;
- Full details of assumptions and limitations of the plan including details of residual risks.

This plan should be kept throughout the project and will probably change over time. All changes should be evaluated and presented to the project steering committee for approval, so the risks are being monitored at an appropriate level. (Government of Tasmania 1998)

Risk management reports should be appropriate to the size, nature and phase of the project. Risk management documents and reports include (Bahnmaier et al 2001) :

Risk Information Form (RIF)

This form has a dual purpose: firstly to provide a source for data entry information and secondly as a report containing basic information. The report provides the team members of the project with a format for reporting any risk-related information. This report is constantly updated over time, as more information becomes available, as well as being refined when potentials risks are identified.

Risk Assessment Report (RAR)

This report is delivered by the teams who have assessed a risk event and amplifies the information given in the risk information form (RIF). The risk assessment report documents the identification, analysis process and results. All information that has been summarised in the RIF is shown in the risk assessment report. The report provides a basis for developing risk-handling plans.

Risk Monitoring Documentation (RMD)

This document acts as a summary which is used to ensure entry into the database. It also tracks the status of high and moderate risks. The project manager can use this document to produce a risktracking list: an example is information that has been entered into the RIF

Risk Handling Plan of Action

This document has the information that links it to the appropriate RIF. It provides the project manager with information that may be useful when trying to choose the proffered mitigation option. The plan acts as the basis of handling plan summary, which is contained in RIF. RHD describes the examination process for risk handling options and gives the basis for the selection of the recommended choice. Once this has been made, a rationale for the choice may be involved (Bahnmaier et al 2001).

Conclusion

There are always risks associated with a project. The purpose of risk management is to ensure levels of risk and uncertainty are properly managed. All projects require a degree of risk management but the effort expended will depend on the scope and proposed outcomes. A successful risk management practice is one in which risks are continuously identified and analysed for relative importance.

Bibliography

Akintoye, S. A., and MacLeod, J. M., (1997) "Risk Analysis and Management in Construction", International Journal of Project Management. Vol. 15, (1), pp 31-38

Ansel J. and Wharton, F., (1992) Risk Analysis, Assessment and Management, Wiley. pp4-5.

Barkki H, Rivard S, Talbot J., (1993) "Toward an Assessment of Software Development Risk", Journal of Management Information Systems. Vol 10, (2), pp203-225.

Boehm, B., (1991) "Software Risk Management: Principles and Practices", IEEE Software 8(1), pp. 32-41.

Bahnmaier, B, Mcmahon, P., Risk Guide For DoD Acquisition. Fourth Edition February 2001

Carnegie Mellon University (2001) Software Engineering Institute http:// www.sei.cmu.edu/ programs/ sepm/ risk/ risk.mgmt.overview.html accessed on 7th March 2001

Decisioneering, Inc 2001 Risk Analysis Overview http:// www.cbpredictor.com/ risk-analysis-start.html accessed on 11th March 2001

Government of Tasmania (1998) Project Risk Management http:// www.go.tas.gov.au/ projman/ projrisk.htm# accessed on 11th March 2001

Haimes, Y., Risk Modelling, Assessment and Management. 1998. pp4-5, 20.

Hall, E., Risk Management Map.1998. http:// www.dacs.dtic.mil/ awareness/ newsletters/ technews2-2/ map.html accessed on 15th March 2001

Holt, G. Software Risk Management - The Practical Approach Mei Technology Corporation http:// www.dacs.dtic.mil/ awareness/ newsletters/ technews2-2/ practical.html accessed on 15th March 2001

McNamee D., 1997 The New Risk Management http:// www.mc2consulting.com/ risknz.htm accessed on 11th March 2001

Pender, S., (2001) "Managing Incomplete Knowledge: Why risk management is not sufficient, International Journal of Project Management. Vol. 19, (2), pp 79-87.

Pfleeger , L., Software tech news Assessing Project Risk- University of Maryland http:// www.dacs.dtic.mil/ awareness/ newsletters/ technews2-2/project.html accessed on 14th March 2001

IRMA MEMBERS' BENEFITS DISCOUNTS

Mark Smith

We have negotiated a range of discount for IRMA members, see below:

A new discount we have added is a 10% discount off all courses offered by E-tec. E-tec offer a range of general and product-specific IT security course and their website (www.e-tecsecurity.com) is well worth a visit.

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
Audit SuperStrategies (www.mistieurope.com)	15%	Lisa Davies (LDavies@mistiemea.com)
E-Tec (www.e-tecsecurity.com)	10%	Margaret Mason (info@e-tecsecurity.com)
Internal Audit & Business Risk (www.iir-conferences.com/iacon)	20%	Jonathan Harvey (jharvey@iirltd.co.uk)
Sarbanes-Oxley summit (www.mistieurope.com)	15%	Lisa Davies (LDavies@mistiemea.com)
All Unicom events (www.unicom.co.uk)	20%	Julie Valentine (julie@unicom.co.uk)

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

BCS MATTERS!

Professionalism in IT

The BCS Professionalism in IT programme, which was the main subject of this column in the last edition of this newsletter, continues to move forward. The Steering Board for the programme met for the first time in September and approved a programme of work designed to produce a clearly defined vision for an IT profession that will meet the needs of all its stakeholders. That work is being progressed by the Executive Board for the Programme, chaired by President Charles Hughes, which also met for the first time in September. The current work plan has 6 main strands of research activity, looking in detail at:

1. The scope of the IT profession
2. Customer requirements of the profession – particularly in terms of the requirements of IT employers and their customers.
3. Comparison between the IT profession and other, more established professions.
4. The competence architecture required for the profession
5. The essential attributes of a standard professional qualification for IT
6. The role, responsibilities and qualifications for senior IT position, such as IT Director and Chief Information Officer.

The Executive Board is due to report to the next meeting of the Steering Board January and to produce final reports in April in time for a major conference on IT Professionalism scheduled for 8th May.

The programme continues to attract very high level support from across the industry with Steering Board representation, at CEO levels from organisations such as Fujitsu, Oracle, Intel, CSC, Accenture, Tesco, NCC and the Office of Government Commerce. Even Bill Gates had good things to say about the programme when he spoke to an ELITE group audience in October:
"I'm an honorary member of the BCS and proud of that, Microsoft is also pleased to be working with BCS on its very important Professionalism in IT programme."
Praise indeed!

BCS moves towards open CITP

Plans to open up the Chartered IT Professional (CITP) qualification to other institutions under licence are also moving ahead. These plans are designed to produce a single, industry-wide chartered qualification recognised as the 'gold standard' professional accreditation in IT. At the present time only the BCS is able to award CITP and membership of BCS is an essential requirement for those holding the qualification. Under the new proposals, it would be open to other institutions to apply for a licence to operate as an awarding body in relation to their own members.

The creation of a single major qualification is seen as essential if we are to create a widely recognised IT profession. It will of course require a change to the BCS Charter and must first be approved by the membership at an extraordinary general meeting (EGM). No date has yet been fixed for the EGM but it is likely to be around the middle of next year.

New Version of SFIA

Following very extensive industry wide consultation, the SFIA Foundation, has launched a new version of the Skills Framework for the Information Age (SFIA).

First published in 1999 as NISFF (National Information System Skills Framework), SFIA has evolved to become the industry standard for IT skills management. It has also been adopted by government as part of its drive to build and develop the newly formalised government IT profession. It is now owned and maintained by a foundation with 4 members – BCS, IEE, eSkills UK and IMIS.

The new version, SFIA 3 is the result of a wide range of input from government and industryThe framework now identifies a comprehensive range of 78 IT skills, and has developed considerable extra strength in the areas of business change, outsourcing management, service management, information management and governance. In addition to these, many descriptions have been improved in the light of the considerable experience that has been gained from widespread use of SFIA.

To complement the new SFIA version 3, BCS will be updating its own SFIAplus3 IT skills, training and development standard which will completely align with SFIA's comprehensive skills sets with additional detailed overviews. It will offer links to specific BCS training, development and qualifications, careers and jobs, relevant professional bodies, standard codes and practices, communities and events, publications and resources. SFIAplus3 is scheduled for release in early 2006.

The 2005 AGM - A New BCS President

At the 2005 AGM, held at the BCS London HQ in October, Charles Hughes became the Society's 45th President, succeeding David Morris. Charles is, a prominent IT professional with an extensive background in both the private and government sectors. He became a BCS member in 1974, a Fellow in 1990 and was elected Vice President Member Services in 2001 and Deputy President in 2004. He served on the Strategy Review Panel from 1988 and led the re-branding work which produced the current BCS logo. Over the past few years he has taken a very active interest in the various moves to improve professionalism and is the Sponsor for Professionalism Programme.

Charles is a Court Assistant of the Worshipful Company of Information Technologists, Programme Executive of the Parliamentary IT Committee, a past Member of the Spectrum Management Advisory Group, past Council Member of the Institute for the Management of Information Systems and past Chairman of the Real Time Club.in IT.

Charles founded eManagement Ltd in 1999 providing strategic and project services to government and the IT industry. His 38 year career in IT began with ICL where he held directorships of marketing, sales and strategic planning and was technical director and purchasing director. As Project Director at the DTI in the 1990's he developed and launched the Information Society Initiative and represented the government in the UK, Brussels and elsewhere. In this role he liaised with the BCS and gained DTI support for ECDL in its early stages.

And a very successful Year

The AGM also received a report of another very successful year for the Society, with overall revenues up by 10% and a very significant increase in membership.. Membership recruitment activity continues to bring in around a 1,000 new members a month and during the year to the end of April we attracted 14,164 new members against the objective of 10,000. The overall result is that, after several years of pretty flat growth, we have gone from 36,828 members at the end of April 2004 to a net of 47,763 at the end of April 2005.

ECDL, now with over 1.3 registered users, continues to grow as also does ISEB which now has more than 50,000 examination candidates per year. And just to add a few more noughts the BCS sponsored scouts badge, started almost a year ago, has been awarded to over 120,000 boy and girl scouts..

BCS Review 2006

Each year the BCS Review brings together the most up-to-date thinking and practical experience of industry professionals on a variety of topics facing the IT community. The 2006 Review which has now been published continues that pattern with analysis of the current concerns and threats within the IT industry and practical solutions to combating common problems, such as IT governance and compliance, implementing VoIP and managing the risks of electronic communications. It also includes a chapter on online fraud prevention and passwords pitfalls, which examines next generation authentication software and recommends the use of wireless mobile devices to generate access PINs for each authentication event.

Other articles in the Review cover:

IT Strategy
IT Training and Education
Software Testing & Solutions
Professional Issues
IT Services
Networks
Application Development Tools
Mobile Computing
Data Storage
Electronic Publishing
The British Computer Society

And Finally...........

BCS itself is on the move. Having moved the London base very successfully last year it is now the turn of Swindon. Almost all BCS staff are located in the town but the split between two buildings is less than ideal. So we are about to leave both buildings to move to North Star House on the other side of the main railway line. Moves start in December and are due to be completed by early February.

HUMOUR PAGE

Mensa, I once again asked members to take any word from the dictionary, alter it by adding, subtracting, or changing one letter, and supply a new definition. Here are this year's (2005) winners:

1. **Intaxication:** Euphoria at getting a tax refund, which lasts until you realize it was your money to start with.

2. **Reintarnation:** Coming back to life as a hillbilly

3. **Bozone (n.):** The substance surrounding stupid people that stops bright ideas from penetrating.
   The bozone layer, unfortunately, shows little sign of breaking down in the near future.

(Wonder what 4 was? Probably a naughty one :-)

5. **Cashtration (n.):** The act of buying a house, which renders the subject financially impotent for an indefinite period.

6. **Giraffiti:** Vandalism spray-painted very, very high.

7. **Sarchasm:** The gulf between the author of sarcastic wit and the person who doesn't get it.

8. **Inoculatte:** To take coffee intravenously when you are running late.

9. **Hipatitis:** Terminal coolness.

10. **Osteopornosis:** A degenerate disease. (This one got extra credit.)

11. **Karmageddon:** It's like, when everybody is sending off all these really bad vibes, right? And then, like, the Earth explodes and it's like, a serious bummer.

12. **Decafalon (n.):** The grueling event of getting through the day consuming only things that are good for you.

13. **Glibido:** All talk and no action.

14. **Dopeler effect:** The tendency of stupid ideas to seem smarter when they come at you rapidly.

15. **Arachnoleptic fit (n.):** The frantic dance performed just after you've accidentally walked through a spider web.

16. **Beelzebug (n.):** Satan in the form of a mosquito, that gets into your bedroom at three in the morning and cannot be cast out.

17. **Caterpallor (n.):** The color you turn after finding half a worm in the fruit you're eating. And the pick of the literature:

18. **Ignoranus:** A person who's both stupid and an ass.

Why computers crash

If a packet hits a pocket on a socket on a port, and the bus is interrupted at a very last resort, and the access of the memory makes your floppy disk abort, then the socket packet pocket has an error to report.

If your cursor finds a menu item followed by a dash, and the double-clicking icon puts your window in the trash, and your data is corrupted cause the index doesn't hash, then your situation's hopeless and your system's gonna crash!

If the label on the cable on the table at your house, says the network is connected to the button on your mouse, but your packets want to tunnel to another protocol, that's repeatedly rejected by the printer down the hall.

And your screen is all distorted by the side effects of gauss, so your icons in the window are as wavy as a souse; then you may as well reboot and go out with a bang, 'cuz sure as I'm a poet, the sucker's gonna hang.

When the copy on your floppy's getting sloppy in the disk, and the macro code instructions is causing unnecessary risk, then you'll have to flash the memory and you'll want to RAM your ROM, and then quickly turn off the computer and be sure to tell your Mum!

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.

It is the Group's intention to move substantially to electronic communication, including circulation of the Journal. Please tick this box to indicate you agree to be contacted this way. □

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE:
(STD Code/Number/Extension)

E-mail:

PROFESSIONAL CATEGORY: (Please circle)

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

SIGNATURE: DATE:

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

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

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
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
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
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
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
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
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
2 = External Audit
3 = Data Processor
4 = Academic
5 = Full-Time Student
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	brewer.alex@gmail.com
SECRETARY	Siobhan Tracey	siobhan.tracey@booker.co.uk
TREASURER	Jean Morgan	jean@wilhen.co.uk
MEMBERSHIP	Ross Palmer	ross.palmer@hrplc.co.uk
JOURNAL EDITOR	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 – ISACA	Ross Palmer	ross.palmer@hrplc.co.uk
MARKETING	Wal Robertson	williamr@bdq.com
ACADEMIC RELATIONS	Vacant	

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

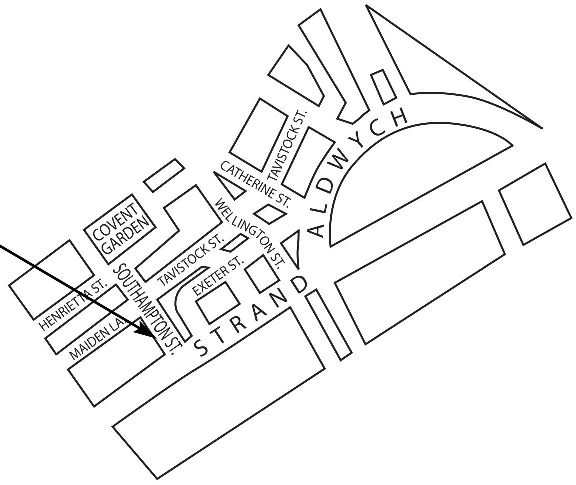
Janet Cardell-Williams,
49 Grangewood, Potters Bar, Hertfordshire EN6 1SL
Email: admin@bcs-irma.org
Website : www.bcs-irma.org

BCS IRMA Specialist Group Advertising Manager

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

Venue for Full Day Briefings

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


TAVISTOCK ST.
CATHERINE ST.
ALDWYCH
COVENT GARDEN
WELLINGTON ST.
TAVISTOCK ST.
EXETER ST.
HENRIETTA ST.
SOUTHAMPTON ST.
MAIDEN LA.
STRAND