ISSN 0961-9348

casg Computer Audit Specialist Group

JOURNAL

VOLUME 6 NUMBER 2 AUTUMN 95

The British Computer Society

Technical Briefings for 1995/96

Tuesday 16th January 1996

Information Highways: The Opportunities for Good and Ill

Chairman: **Lynn Lawton**, KPMG

Speakers: **Geoff Cox**, Micro Active

Dr Roger Wallis, City University

Trevor Williams, Clarke Whitehill

Tom Mulhall, Manager of Detective Operations, BT

Organisers: Geoff Wilson - 01962 733049

Jim Ewers - 01992 555328

Tuesday 16th April 1996

"Readiness is All": Making better use of the Technology

Chairman: **Judith Scott**, Chief Executive BCS

Speakers: **Graham Clukas**, Price Waterhouse

John Ford, Quality Methods Manager (IT), Safeway Stores plc

Sue Mathews, Training by Design

Stan Dormer, System Security Ltd.

Organisers: John Bevan - 01992 582439

Diane Skinner - 0117 923 6757

Tuesday 16th April 1996 16.30

ANNUAL GENERAL MEETING

Technical Briefings are held at the Royal Aeronautical Society (see back page).

For last minute confirmation contact the relevant organisers.

The ***Journal*** is the official publication of the Computer 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

Designed and set by Carliam Artwork, Potters Bar, Herts
Printed in Great Britain by Dodimead Ball, St Albans, Herts.

EDITORIAL

No volunteers came forward to offer to edit the proposed 'restaurant & hotel watch' column. I suspect the reason being that none of you want your organisations to know what a good time you are having at their expense. Never mind, I will now keep to myself that little place I know in Amsterdam which serves smoked salmon and champagne as part of its normal buffet breakfast! No letters to the editor either. Is there anyone out there?

On the content front this edition we conclude the Leemings' three part article on secure systems. Those of you of an observant nature will notice that we have swapped the precedence of the names of the two authors. This is as a result of a conversation that I had with Anne Leeming during which she pointed out that Geoffrey had done all the real work for the article and should receive the appropriate recognition. In this day and age of cut-throat academia publishing I thought it particularly nice of Anne to give such recognition to her co-author.

We are also starting another refereed three part series, this time by George Allen of Portsmouth University, on how to estimate the time, cost and resource requirement of a software development. This is a particularly weighty series, but it should be compulsory reading for all computer auditors as it provides the tools to check the estimates made by the IT professionals. As most systems come in late and over budget it is important that we do all we can to help our organisations to get their estimates correct in the first place.

You will also find a raft of product and books reviews, plus a couple of member profiles and news from the BCS, including a new regular column dealing with the IEE library which you are entitled to use. The editorial panel is working well, but if you have any ideas for additional columns, or if you are willing to help edit such a column, then please let me know. After all, this is your Journal.

John Mitchell

Contents of the Journal

Chairman's Corner

Alison Webb

"The world is too much with us; late and soon,

Getting and spending, we lay waste our powers."

What would Wordsworth have thought about E-Mail and the Internet? He obviously wouldn't be as positive as we are: to us, being in touch is really important, and mobile phones, faxes and E-Mail are essential accessories for anyone really serious about doing business. Perhaps partly we just welcome what's available: in the same way, we place far more emphasis on washing and personal hygiene than our ancestors who had no en-suite bathrooms and didn't know about the Body Shop,

Yet Wordsworth does have a point. It's clear that the more communicating we do, the more time we spend sifting information and trying to decide what merits attention. Is what we collect worth the effort of the sifting? President Clinton obviously thinks not: he has commissioned software to read his E-Mail and compose and return standard replies, without any human intervention. A recent *Times* article I read suggested that some firms withhold information from people compiling directories simply to reduce the avalanche of irrelevant letters they receive.

We also think better if uninterrupted. Copernicus produced his best work more or less isolated in a Prussian tower; Newton had his ideas for the Principia not a Cambridge, but far from his colleagues in his garden at Woolsthorpe. If we spend all our time reading and writing messages and answering the phone, won't our productive output suffer?

This isn't a new problem, of course: people have always had to balance the requirement to be accessible with their need for some privacy and time for reflection. People are already starting to put filters on their availability: I have already seen one demand for written responses only to a proposal: no fax or telephone number supplied, let alone an E-Mail address; and lots of people, of course, are already selective about the phone calls they return.

So do we make any real progress? Well, as far as I'm concerned, it can't just be cultural conditioning that means I prefer washing in a centrally-heated bathroom than under the pump in the back yard: and the same is true of communication. I like being able to talk to and exchange messages easily with people at the other end of the earth. I do see, though, a great future for sieves: ways of extracting nuggets of interest from a mass of largely irrelevant rubbish.

This is something that relates neatly to our work as auditors. We are already great advocates of the filter, for security purposes: we can now reinforce our arguments on VFM grounds as well. Checking the identity of a potential E-Mail correspondent will soon, perhaps, be not just to rule out hackers, but also to see if he or she is likely to have anything interesting to say. So E-Mail messages from my creditors will be returned automatically as 'address unknown', while calls from potential customers get straight through. But this sounds familiar: isn't this sort of filtering exactly what secretaries have been doing since the invention of the telephone? And wasn't E-Mail supposed to be better because it removed such barriers to communication?

No wonder courier services are on the increase: how can you sieve envelopes?

Guidelines for Potential Authors

The Journal publishes two types of article: refereed and invited. Refereed articles should be technically oriented and based on current or future issues related to information systems audit, security or control. This type of article will be reviewed by at least one member of the editorial panel (anonymously). If published, it will be identified as a refereed paper.

An invited article need not be technical or overly academic (even Computer Auditors have a sense of humour!) In fact it need not even be 'invited'. Submission without invitation is encouraged and although this may lead to severe sub-editing by the Editor, submission will virtually guarantee publication.

We also invite members to volunteer for book, product and course reviews (anonymously if required).

Why not call John Mitchell (Tel: 01707 851454, Email: jmitchell@lhs.win-uk.net) to discuss how you can get your name in print.

Abstract

Companies with sensitive or critical systems face two main problems: no computer security measure can ever be 100% effective, and highly secure systems are highly expensive. This paper poses the benefits of the holistic approach, whereby an integrated, 'across-the-board' security policy is implemented, rather than specific measures to counter specific perceived threats. The holistic approach is shown to benefit security by providing a high level of security for a relatively low cost. A security evaluation model, the 'Five Shields' model, is created to show up vulnerabilities of security policies and assess the strength of protection provided.

Secure Systems in the Finance Industry – The Benefits of a Holistic Security Policy

(Part 3 of 3)

G.S. Leeming and A.M.C. Leeming

5. The 'Five Shields' Model

The five shields model has been designed by the authors to check how well balanced a security policy may be. It provides a graphical representation of the spread of the security countermeasures, and compares these against the spread of the perceived threats to the system. The model is entirely qualitative. Security is not a field in which it is easy to be accurately quantitative, as it deals with a high degree of estimated probabilities and value judgements.

The model is presented in the form of arrows aiming at a target, which is defended by five shields. The integrity of a company's systems is represented as the target for which the arrows, representing the possible threats, are aiming. Between threats and integrity lie the five shields, representing the five areas of security countermeasures described in section 4. Note, however, that quantification measures are not a direct defence against any threat, in that they only help to comprehend the problem. Therefore the first shield is placed in the second line of defence.

To use the model, it is essential first to decide which system's security is being considered, and write that in as the target at the head of the page. Then add in the five shields, and within each shield, list the relevant security countermeasures. For instance, if the company in question operates access control mechanisms, then 'access control' is listed in the 'Defence Mechanisms' shield. Then, the mechanisms that rely on each other are linked by lines to indicate their interdependence. For example, an access control measure which relies entirely on the user identification measures in place: it is no use limiting a particular employee to certain information, if that employee can successfully pose as another employee in order to gain access.

When all countermeasures have been listed, a graphical representation of the spread of security measures is obtained. This can be used to indicate whether or not the subject's security policy is balanced. For example, if many more measures are listed under Defence Mechanisms than under Personnel Measures, then the company is not operating a balanced policy.

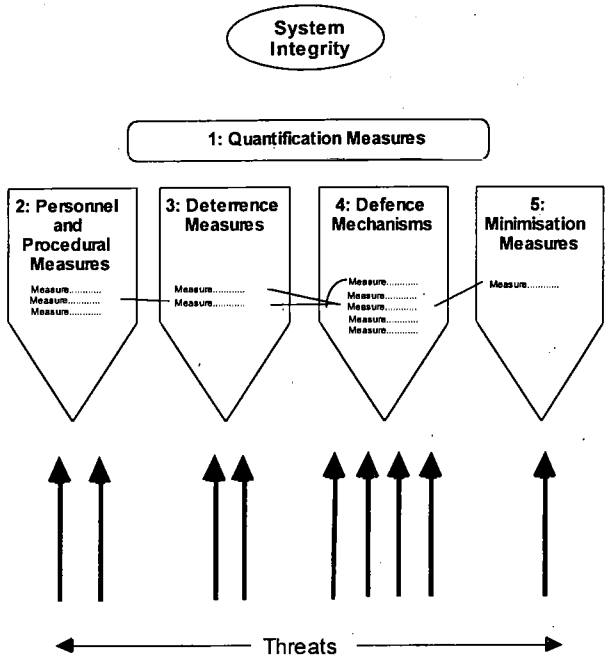
It is important to consider the balance of the policy before embarking on the next step, which is to add the perceived threats and compare them with the listed countermeasures. It is more efficient to have a balanced policy, even if some of the measures may not seem immediately applicable. This is for two reasons: firstly, because new threats will develop which will take advantage of weaknesses in the defences of the system, and secondly, because of the synergistic effect of having a balanced policy. This point will become clearer when seen in action in the case study (q.v.).

The next step is to add arrows beneath the shields to represent the threats to the system. For each threat, one arrow is added under each shield which may be expected to prevent it. For example, one such threat could be hacking from external sources. An arrow is added under the defence mechanisms' shield and the minimisation measures' shield, but not the personnel or deterrence shields, as personnel measures do not affect external sources, and hacker attacks do not normally come into contact with deterrence measures.

When all the likely threats have been added, the problem can be considered in four separate parts. the measures listed in each shield can be compared with those threats marked underneath that shield. This splits the problem into more readily comprehensible sections. An evaluation of the strength of the listed measures within each shield against the strength and likelihood of each threat will reveal any flaws in system security.

The basic diagram is shown overleaf (Figure 5.1.)

Figure 5.1. The Five Shields Model



Case Study: Chelsea Ltd.

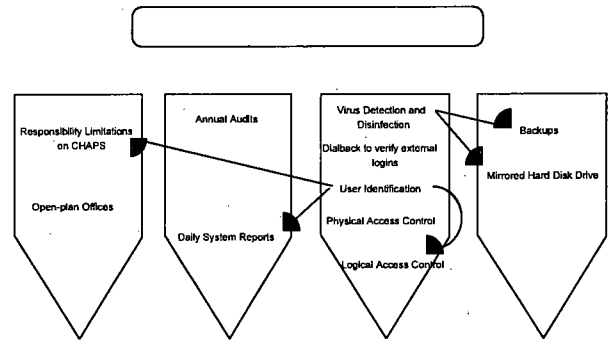
For the purposes of this exercise, I shall only consider Chelsea's main system, the office automation suite. There are security risks associated with the TOPIC3 stock quotation system, primarily that of denial of service, but they are less wide-ranging than those affecting the office automation system.

Considering the security already in place area by area, one can see that Chelsea run the following countermeasures:

Quantification	None
Personal and Procedural	Open-plan ofices
Deterrents	Annual audits by external auditors – Daily System reports
Defence Mechanisms	Access control Virus Disinfection Dial-back verification for external users User identification – user-id/password Physical Access Control
Minimisation	Backups Mirrored hard disk drive

The interdependencies are few in this case: most measures depend on the user identification mechanism, which unfortunately is the weakest link of the entire system. Sharing responsibility for CHAPS transfers between three people is laudable, but while passwords are shared, any person can pose as the other two people required. System reports of irregular events are of little use to the system manager if he cannot trust in the reports from which 'user-id' the irregular event originated. Access control measures are similarly compromised. A lesser interdependency is that between the anti-virus measures and the backup procedures and mirrored hard disk. If the anti-virus measures do not work, then in the event of a virus attack, it is likely that recent backups will also have been infected.

Thus, when added into the model.....



There are two glaring imbalances here: the complete lack of quantification measures, and the preponderance of defence mechanisms. These are common features of security policies, especially in finance and especially in small to medium sized companies. The policy is unbalanced: it is not possible to tell whether or not it is effective until some quantification measures are in place.

Next, the threats should be considered. Again, without quantification measures such as risk analysis, the following will not be the canonical list, nor can relative likelihoods be determined. However, these are the most significant threats:

1. Fraudulent use of CHAPS

2. Virus attack

3. Physical damage to site or hardware

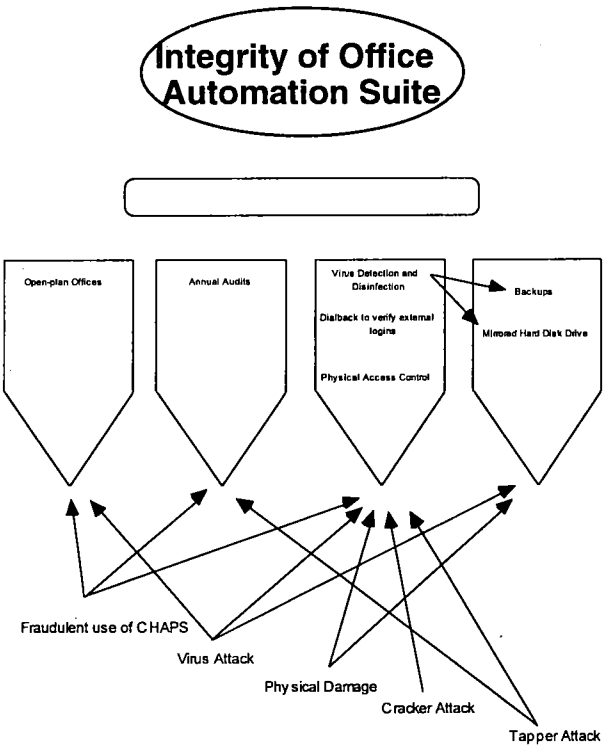
4. Cracker attack, with no further criminal intent in mind

5. Tapper attack against commissions records

When confronted with these threats, it is clear that the user identification procedure is no realistic defence. It would be very simple to crack, owing to the shared passwords, and like a latch lock on a window, it deters only the curious. It poses no defence against an intruder

with any determination, such as threats 1, 4 and 5 above. Therefore the user identification measure can be removed from the countermeasures list. This means that the measures that rely on it are compromised, and can themselves be removed.

Adding the three parts together, we obtain the completed model:



This final picture gives a far clearer indication of the security situation at Chelsea than words can: relatively few major threats, but in practicality, almost no defences. Now we can consider the situation area by area.

Personnel and Procedural Measures

Personnel and procedural methods which are in place to prevent a potential multi-million pound fraud on CHAPS amount to nothing more than an open-plan office, where everyone can keep a vague eye on each other. This would be a minor inconvenience to a fraudster, and nothing more.

P&P measures can be implemented to guard against virus attack, namely a policy of insisting that unauthorised software, such as games and shareware, must not be used on company machines. However, no such procedures are in place.

Deterrence Measures

Deterrents could be put in place to guard against both the potential CHAPS fraud and a Tapper attack. However, the only remaining measure, the annual audit, is far from sufficient. It is too infrequent and too general to stop either threat: indeed, that is not its main aim.

Defence Mechanisms

This area is where any of the threats can be stopped. There are three remaining measures in place: anti-virus measures, the dial-back system, and physical access control. Each of these three measures are good, and do a lot to rescue the company's security.

The anti-virus package works by recognising and flagging known viruses - its weakness is that it cannot detect new viruses, though it is updated regularly. The dial-back system almost entirely eliminates the cracker problem at a stroke. It is possible to confuse a dial-back system into calling an unlisted number, but it is not easy. The physical access controls are weak, but sufficient to stop the opportunistic or petty thief/vandal.

However, none of the defence mechanisms address the two most serious threats, the CHAPS fraud and the Tapper attack on the commission records.

Minimisation Measures

The two measures in place here, the mirrored hard disk and the backup procedure, are two different methods of doing the same thing. They both minimise data loss in the event of a virus attack or a physical breach.

No minimisation measures are in place against the CHAPS fraud or the Tapper attack. However, neither threat is easy to minimise without affecting the company's operational capability.

Recommendations

Chelsea have managed to protect themselves against the minor threats, such as theft, cracking, and viruses, but have signally failed to implement any workable protection against the two serious threats facing them, a CHAPS fraud and the loss of confidentiality of the commissions record.

It is a simple enough matter to identify the largest vulnerabilities in the company's security. Chelsea can improve their security vastly for a relatively low cost in time, effort and money.

Firstly, the user identification mechanism should be completely replaced with a more effective mechanism[13], individual passwords should be assigned, and passwords treated as confidential. Once this mechanism is working effectively, the responsibility limitations, access control measures and daily system reports will again become valid. The responsibility limitations and access control measures form a moderately effective defence against fraud, and the identification mechanism itself forms a good defence against crackers, if used properly.

[13] For example, one which has a longer minimum length of password, more complex usernames, requires regular password changes, and refuses to accept 'Dictionary' words as valid passwords.

Secondly, the IT manager and the Managing Director should jointly issue a security policy document (q.v. 4.3). This measure costs the company very little and can bring great benefits. Ideally, the document should be issued concurrently with the introduction of the new user identification mechanism. Then both improvements will support each other: the new passwords will assure the employees that the policy document is more than just hot air, and the policy document will help to ensure that employees keep their passwords confidential.

These two measures will restore Chelsea's security to a functioning state. It will then have a holistic policy covering four of the five areas, offering some protection against all threats. The next stage is to determine what is the optimum level of security for the company, i.e. the appropriate level of security to counter all expected threats. For this, Chelsea needs to carry out a thorough and formal risk assessment on their systems to determine what the possible threats are, and what they might be expected to cost the company. Once the risk assessment is in place, the fifth of the five areas will have been covered, and Chelsea will have sufficient information to re-run the five shields model, and view support or counter its recommendations with financial arguments.

Conclusions

As was described at the beginning of part one, the holistic approach is clearly part of the next generation of security. Integrated, planned, proactive systems provide better security more efficiently than 'bolt-on', ad-hoc systems. Security is something that needs to be taken seriously, and so a security policy must also be taken seriously.

The strongest, and most elusive, benefit of the holistic approach is that it builds up a culture of security. This culture of security, as has been explained above, supports the operation of all security measures, and helps protect the integrity of a company's systems. As with 'corporate morale', the security culture is very difficult to define and quantify, and its benefits are just as difficult to measure. The specialised approach to security (q.v.) tends to not encourage this culture (DeMaio, 1992), and it is very difficult to artificially force such a state of mind on personnel.

Synergistic effect is what makes the holistic approach different from the specialised approach, but it is often very difficult to see in advance just what measures will complement each other. Synergy, as with the security culture, is a 'soft' force, and is not easy to design or artificially induce. It is not easy to plan synergy; it is something which occurs following no rules. This is where the five shields model comes in useful. It shows which measures support each other, and helps to build an overlapping policy. These are the conditions where synergy can occur.

The major weakness of the Five Shields model is in that it does not place sufficient importance on 'strength of mechanism', i.e. the ability of the mechanism to do its job effectively. The model cannot distinguish between a simple password algorithm, for example, that allows single-letter passwords and which doesn't enforce changes, and a rigorous algorithm that places calculated restrictions upon passwords to improve security.

During the final stage of the model, perceived threats are compared against countermeasures in place, but it is left entirely to personal judgement as to how to compare the two. Some formal means of comparison, such as CRAMM, needs to be added to the model to cover this deficiency. However, this would need to be carried out in conjunction with a formal means of investigating the threats; this investigation and comparison is formalised in risk assessment methodologies. If the Five Shields model is run in conjunction with such a methodology, the deficiency will be covered.

It is worth comparing the model with the Optimum Mix of Controls (OMC) methodology (Burch and Grudnitski, 1989). Both methodologies aim for the same result in a different manner. The five shields model is an entirely qualitative model, supporting personal judgement, whereas the OMC method is entirely quantitative, 'formalising' personal judgement.

The OMC works by estimating a potential loss range for each possible hazard, along with the level of exposure, or probability that the hazard will occur. Using these figures, it produces an expected average cost per year of security threats. It then compares this with possible countermeasures, modified by their percentage risk of failure, to determine the optimum mix of controls.

The first advantage OMC has over the Five Shields model is that it takes strength of mechanism into account when determining the optimum mix. It provides no means of determining strength of mechanism, but it does have a place for the estimated percentage risk of failure of each mechanism. This, with slight modification, could be used as a strength of mechanism measure.

But the most fundamental difference between the two is a result of the difference in approach, quantitative vs. qualitative. Whereas the Five Shields model supports judgement, but comes up with no definitive answers, the OMC method constrains judgement, by using it only to provide estimates of value and probability, but does come up with a definitive answer. It does not address the view that no definitive true answer can be believed in such an unpredictable field as security.

The OMC method also relies very heavily on estimates: estimates of amounts of losses; probabilities of hazards occurring; probabilities of mechanisms failing. Some form of risk assessment lies at the heart of any security policy design tool, and therefore all such

tools rely on estimates. However, the OMC method uses these estimates and builds them into a concrete answer. There is a fundamental problem with estimates of values of IT systems: it is very difficult to put a price on a system. It is easy to price the investment in the system, but not to measure its value to the company. How do you price data? Do you include training costs, personnel costs, overheads, etc.?

Its final flaw is that the OMC method has no place for the 'soft' defences: personnel and procedural measures; quantification measures; and deterrence measures. Such measures cannot be given a percentage chance of failure, and cannot be expected to succeed every time. Their effect cannot easily be quantified, and therefore they cannot easily be included in a quantification model.

In comparison to OMC, the Five Shields model's biggest drawback is its vagueness. It does not attempt to provide a definitive answer, and it could be seen to add little to the problem. But the model is a high-level framework to aid personal judgement, not a 'recipe'-like methodology that will replace the experience of a skilled professional. It is most useful as a tool for the security manager; as a 'soft' methodology to complement, rather than replace, the 'hard' methodologies of risk assessment and Burch and Grudnitski's OMC.

7. References

Alderton, A.D.D., **What Price Security?**, 1991, CIBA-GEIGY Plc.

alt.security, Internet News, 1990-1994

Baskerville, R., **Designing Information Systems Security**, 1988, John Wiley Ltd.

Burch, J.G., and Grudnitski, G., **Information Systems**, 1989, John Wiley Ltd.

C.C.T.A., **An Overview of CRAMM**, 1990, HMSO

Cornwall, Hugo, **Hackers Handbook**, 1985, Century Communications

Cornwall, Hugo, **Industrial Espionage Handbook**, 1992, Ebury Press

Corrupt Computing Bulletin Board, 1990-1991, 0203 768311

DeMaio, Harry B., **Information Protection and Other Unnatural Acts**, 1992, AMACOM

Earl M. J., **Management Strategies for Information Technology**, 1989, Prentice Hall

Hafner, K. and Markoff, J., **Cyberpunk**, 1991, Fourth Estate Ltd.

Hoffman, Lance J. (ed.), **Rogue Programs: Viruses, Worms, and Trojan Horses**, 1990, Van Nostrand Reinhold, New York

ITSEC in the Commercial Market, 1994, Kingston University Business School Consultancy Projects

Jenner, P. (Ed.), and Rentell, M. E , **Breakdowns in Computer Security**, 1991, Computer Weekly Publications

NCC Consultancy, **IT Security Breaches Survey Report**, 1991

Norman, A.R.D., **Computer Insecurity**, 1983, Chapman & Hall

Sherman, Robin L., **Electronic Banking Security**, Datapro Reports on Information Security, 1991, McGraw-Hill

Sterling, Bruce, **The Hacker Crackdown**, 1992, Penguin Books Ltd.

Cranny, Mark, **The Detection and Prevention of Computer Based Crime**, May 1988, City University Business School

Shapira, Paul, **Competitive Overview of the Secure IT Market**, October 1992, ICL Internal Report

Warman, A. R., **Organisational Computer Security Policy: The Reality**, European Journal of Information Systems Vol. 1, No. 5, pp305-310, 1992

Wong, Dr. K. K., and Farquhar, W. F., **Computer Crime Casebook**, August 1983, BIS Applied Systems

Appendix A – Chelsea Ltd. Case Study

This case study is being used as an illustrative example for this paper only, and is not meant as an illustration of good or bad security practices.

Nature of Business

Chelsea Ltd. is a small stockbroking firm with under 200 employees. Its head offices are in the City of London, and has smaller offices situated around England and Scotland. The IT Department consists of an IT Manager and three staff, whose duties consist of technical support and simple analysis and programming. This case study is based on an interview conducted with the IT Manager and Managing Director.

IT Systems

The company presently operates two IT systems.

The first is a price quotation network, TOPIC3, linked to SEAQ, the Stock Exchange Automated Quotation system. This system provides up-to-the-second information on share prices in the London Stock Exchange. The system exists only to provide information: the company has no direct means to alter the information contained therein, aside from the influence of their actions within the market. Deals are negotiated and carried out via telephone. All stockbroking companies have a similar or identical system, as it forms a fundamental part of stockbroking operations.

The second system, which is not directly linked to the TOPIC3 system, controls Chelsea's day to day operations. It provides for all the data processing needs of the company, and consists of office and work automation software. The system is leased from an external software house, and is executed on a HP9000 series UNIX mainframe with a 15Gbyte mirrored hard disk drive, based in the London office. The company is not allowed to modify the core software. There are approximately 180 terminals situated throughout the company's offices in the UK. External links are handled via a dial-back system over standard BT lines. The software house has external access to the system for maintenance purposes, with commensurate system privileges. The IT manager does not have access to, or control over, this account.

Of particular note are the system's CHAPS[14] EFT[15] link, and the records of commissions charged. The commissions record is sensitive information: the company believe that if this information were to be released to its clients and/or competitors, then the business would suffer. If competitors were to obtain the information, they would be able to 'poach' their customers by offering a lower level of commission, which could drive the company out of business. Commission rates differ from client to client dependent on what the client will accept. If a client were to discover that another client was being charged at a lower rate, he might either demand a reduction of commission or withdraw his custom entirely.

The CHAPS link contains far greater potential for abuse. The CHAPS system allows users to transfer money between almost any global financial institution. Armed with a basic knowledge of the system, a user could transfer millions of pounds from the company's account to an overseas bank within seconds. However, many banks follow a policy of verbally checking any unusual money transfers. A theft on such a scale would seriously prejudice the company's ability to continue operating.

[14] Clearing House Automated Payment System

[15] Electronic Funds Transfer system

Security Measures

At present, the company operates physical access control, user identification, responsibility sharing, access control and system audit measures.

Physical access control consists of electronic locks controlled by smart cards on the entrance doors to each level of the building. There is no facility to determine whether the holder of any smart card is authorised to own it[16]. The main door is locked at night, but otherwise entrance to the building itself is not controlled in any way. Within each level, offices are open-plan and, as the building is relatively small, anyone on one level can see anyone else on the same level. There is one receptionist on duty during the day, but no security guard. However, the reception desk is located on the ground floor of the adjacent building, and so the receptionist has neither control nor visibility of anyone entering via the main entrance.

User identification measures consist of a *network user identifier* or 'user name' and a password. The user name is set by the IT manager, and is a three-character string comprising the users initials. The password must be a minimum of one character in length. Passwords are commonly shared between groups of workers, and are not treated as confidential. Passwords are changed at irregular intervals at the prompting of the system manager.

The CHAPS link is protected by responsibility limitation measures. Three distinct steps must be carried out in order to transfer money to an external account, and no single user has authority to carry out all three steps. The software house engineers do not have sufficient system privileges to carry out any of these steps.

Not all personnel need to be able to modify data contained in the system in order to carry out their jobs. Data modification privileges are restricted to those users for whom it is required.

The system provides daily reports of the previous day's system events to the IT manager. These reports are provided automatically, and no user has sufficient privileges to suppress parts of the report. Additional reports can be produced upon request.

The system manager carries out irregular and infrequent overviews of the system to check what functions individual users are using.

The company's insurers have carried out a risk assessment on the system. The final report was issued to the Managing Director. The IT Manager has access to the report upon request, but has so far seen no need to do so. The insurers have stated that they are unhappy with the policy of sharing passwords, and have

[16] For example a Personal Identification Number, or PIN

repeatedly recommended that passwords be kept confidential. The IT Manager has no intention of modifying this policy.

Internal View of System Security

Responsibility for implementing security lies with the IT Manager. The Managing Director retains ultimate responsibility, but the IT Manager freely admits that the Managing Director has very little knowledge of IT, and has not yet 'interfered'. The IT Manager believes that the system is as secure as possible. His attitude is summed up by his view that *'if hackers can break into NASA, we cannot stop them breaking into [the company]'*. He also stated that the company has not yet suffered from any significant security breaches. The Managing Director is satisfied with the company's level of security.

The user identification procedure is viewed as sufficient security, despite the password-sharing policy. The IT manager believes that the difficulties of obtaining an employee's middle initial (which forms part of their user name), coupled with the complexity of operating the system, are sufficient deterrent to both internal and external hacking and fraud attempts. It is symptomatic of the lack of password confidentiality that when, during our interview, the system manager logged in to his 'super-user' account he made no effort to obscure my view of his user name or (three-letter) password.

Although he admits that a determined fraudster could put the company out of business, the IT manager is not worried at the prospect. He believes that the fact that the fraud would be reported by the system the following morning, along with the user name from which the fraud was committed, is enough to deter any fraudster.

The external link to the software house is not viewed as a threat to security. The IT manager believes that employees of the software house do not have enough of an in-depth knowledge of the system to carry out a detailed fraud, and further that during the time it took them to write the modifications to the system necessary to avoid detection, he would be bound to notice the extra system activity. He had not considered the possibilities that the very engineers who wrote the system might have a thorough knowledge of its functionality and capabilities, and that system modifications could be performed upon a copy of the software, and the relevant 'patches' uploaded and installed within seconds. After being made aware of these possibilities, he still did not consider the link to be a threat.

The Managing Director stated that currently there were no plans to improve system security.

The Authors –

Geoffrey Leeming *developed an interest in IT Security in Finance as part of his studies at Kingston University Business School. He is currently working in the Computer Audit and Security Group at KPMG and studying part-time for an MSc in Information Security at Royal Holloway College University of London,*

Anne Leeming *is Director of the MBA programme, IT and Management, at City University Business School. Her research is in the impact of IT on organisations and in the way they manage with IT.*

CASG Editorial Submission Deadlines

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

Product Reviews

This regular column, edited by John Silltow, will bring you reviews of products from the control and security arena. John would appreciate any help that you can provide in either reviewing products, or drawing to our attention any software, or indeed hardware, that may of interest to computer audit and security professionals.

PINPOINT 3 FOR WINDOWS

Reviewed by: John Mitchell

Control Self Assessment here I come! No problems for me in helping management to generate those self assessment questionnaires. In fact I will welcome them. What is even better I can supply them with the questionnaires on diskette, get them to complete it electronically and then send it back to the audit castle. There, sitting in my lair, I can import all the completed questionnaires, analyse the results and then sally forth to do battle with the ones I suspect of being not quite kosher. I can also produce beautiful analyses and graphs for my quarterly meeting with my Board Audit Committee. "How goes it Mitchell?", they enquire. "Fine, sirs, fine", I grovel in answer, "But there are a couple of areas that I think we should look at further before our illustrious chairman appends his signature to that Cadbury statement thingy in the annual report. You see this bump on the graph here ....?".

Okay, okay, so once again I let my mind wander, but that is what this package does for me. Knock up a simple ICQ? No problem. Do a complex 15 page questionnaire on disaster recovery with umpteen questions? About a day, and it looks good too. Everything lines up and I can change the questions in a flash.

So about the package. Pinpoint has three main components: questionnaire design, answer input and analysis. Installation is straightforward from within Program Manager and an appropriate icon group is created. The package is well behaved and ran well on both my 8 megabyte 386sx/16 and my souped up 20 megabyte 486/50 machines. The minimum specification is a 4 megabyte 386.

Questionnaire Design

The manual does not attempt to train you in questionnaire design, but it does provide a straightforward and useful guide to the rich facilities available in the system. The on-line help is excellent too, so you will probably only refer to the manual when you start to use the package's capabilities to the maximum. The example files provided are a little disappointing (from the point of view of lifting them directly into a questionnaire), but they do provide useful examples of the facilities available.

The package is not as immediately intuitive to use as say, a word processor, but once you pick up the idea of dragging the question design tool to designate the block of space that the question will occupy, it is quite straight forward. Another, not so straightforward thing is inserting some space between two questions that you have already designed so that you can insert the one that you forgot to do earlier. To do this you have to use the 'insert paper' tool, rather than just position the cursor and hit the return key a few times.

Another irritation is that headers and footers are not supported. I like to put the name of my company and my copyright statement on every page. To achieve this in Pinpoint I have to manually insert them on every page. Okay, this is not too onerous using the copy and paste facilities provided, but if you subsequently insert a few more questions, then you will need to check the position of your headers and footers as they may no longer be performing those roles.

One other thing that foxed me was when I inadvertently 'lost' part of a multi-choice question. One minute it was there and the next it had disappeared. Eventually I worked out that it had slipped off the edge of the page due to some fancy layout editing that I was doing. Could I persuade the blasted thing to come back? No I could not, as I was unable to select it as it was off the paper. In the end I deleted the entire question and re-input it. Something that is very quick to do anyway.

On the whole though, questionnaire design with this package is a lot easier than with a word processing package, although I would have liked to have had a spell checker as there is nothing more irritating to a potential respondent than to find that the word questionnaire is spelt incorrectly on every page! These niggles aside however, I would now rather design my questionnaires with Pinpoint than with my favourite word processor.

And the best bit is yet to come. You can publish the questionnaire either as a standard paper document, or on a diskette with a self executing Windows based program which allows the respondent to complete the questionnaire on their own computer and then return the file to you for automatic import.

Answer Input

This is about as easy as it can be. If you are entering answers from a paper based questionnaire you simply call-up a blank answer sheet and input the results. In many cases you can simply click the mouse over the appropriate box. If you have persuaded your respondents to do the work for you, then you simply import the completed answer sheets directly from the returned diskette. Both methods work well and the result is a 'worksheet' which contains the answers from all the returned questionnaires just waiting for you to analyse.

Analysis

This is where the package really scores over any word processor based questionnaire that you may have used in the past. Pinpoint will take the worksheet and let you analyse the results in a multitude of ways. Graphs are a snip and there are plenty of formats to choose from. You can analyse all the questions automatically, which results in Pinpoint graphing every question that it is possible to graph, or you can selectively choose those questions that are of particular relevance. The resulting graphs can be 'edited' to the extent that you can put sensible names on each axis, play around with the legend, re-scale them and move them about. The resulting 'presentation' can be saved for subsequent retrieval and printing. I used the package to graph 33 responses to 24 questions on disaster recovery into 4 separate presentations. The total time for this, including all my editing time for getting the presentations to look right for my report was about an hour. Not bad for a beginner.

Conclusion

I had previously read a few other reviews of this product where the authors concluded, "Nice package, I am sure that there must be a use for it somewhere". Well there is. Control Self Assessment will require the audit department to help management in the design of ICQs tailored to their particular department. Subsequently, it will be necessary to evaluate management's self assessment against those questionnaires. Take my advice. Get a copy of Pinpoint and become a local hero.

Product	Pinpoint 3 for Windows
Contact	Longman Logotron 01223 425558
Price	£499 for a single user £1,200 for a 3 user site license - extra users £200 each
Good Points	Superb questionnaire design facilities and analysis
Bad Points	Some niggles on the design front, no spell checker
Conclusion	An expensive package which still represents good value for money if you expect to use a lot of ICQs

RITS - Private File version 2.0

Reviewed by John Silltow

This is a small utility product which loads and runs under Windows 3.0 and above. It requires no additional memory to the normal Windows basic configuration but does make the point that the more memory, the faster it runs. It was however only tested on a 4 Mb machine to ensure that it could run in that environment.

It loads from a single diskette and occupies around 800 Kb of hard disk space. It provides four utilities:

1) Encryption/Decryption
2) Configuration
3) Key Management
4) Secure Shredding

The program allows differing levels of encryption to be provided to files. It envisages company-wide, Executive level only and local storage. As all these keys are set up by the Administrator however, data can be recovered if a user leaves. One other option is to enable users to create their own 'personal' key. Data encrypted under these keys could not be recovered by anyone else. Default key sets are provided for the lazy!. The keys can be alphanumeric or hexadecimal and are 8 characters in length. The manual claims the algorithm used to be based on the 'Data Encryption Algorithm' which either means they do not know what DES stands for or it is an unsubtle attempt to pass off their proprietary algorithm as an industry standard one.

The system defaults, as set by the administrator, are stored in an encrypted .INI file uninspiringly called ENCRYPT.INI. This code plus a reduced set of options would have to be distributed to users who will then only see items (1) and (4) from the above list on their desktop. It follows that any machine with this ENCRYPT.INI file could be used to decrypt any documents that machine's user has access to.

In use, the program works with impressive speed. Encrypting and decrypting word processed documents

took under 3 seconds and there were no corruptions of any form. The overhead of encryption on a measured document was minor with an AmiPro document being extended from 9,705 bytes to 9,784 bytes.

I was however very disappointed in that when 'secure erase' option was invoked and yet when I had performed the encryption, the original (unencrypted) document was still readable on the hard disk. Admittedly it had been deleted from the directory tree and I had to view the particular disk clusters it had been in. I was also less than impressed to see the 'restricted drives' option on the configuration screen was not explained in the manual. I believe it enables the entire hard disk to be encrypted at once but would have appreciated the manual's assurance of that and how I could recover from it if it went wrong!

The secure shredding is however excellent. The file involved is overwritten by zeroes and is not therefore recoverable or readable. This is what I believe 'secure delete' should be giving us.

In summary this is an interesting product. I believe the flaw in secure erase is too significant to give it a positive recommendation. It would however need to be used in a secure environment in any event to prevent the misuse of the .INI file and because of this, it may be considered that the ability to see the unencrypted file on the hard disk is an acceptable price to pay.

Product	Private File version 2
Contact	RITS 003531497 3489
Price	£95 with discounts for quantities
Good Points	Multi-level fast encryption processes
Bad Points	Secure erase facility compromises security. Manual does not cover restricted drive option
Conclusions	Good product for an already secure environment

RITS - PC Logon version 2.0

Reviewed by John Silltow

This is a small utility product which loads and runs under DOS to provide access control including boot and file protection.

Loading was an interesting exercise as the INSTALL.EXE program did not run from the A:\ prompt as the manual suggests, but was actually located in the sub-directory A:\DISK1.

After this, when it went to amend my CONFIG.SYS file it failed with 'bad command or filename'. I had to key in the changes through the DOS editor which it did, thoughtfully, provide on screen for me.

I suppose I wasn't then at all surprised to receive yet another message telling me that it was unable to open the C:\RITS.PCL\SIGNON.INI file. Or that the options were retry or abort. I guessed by then that the next message would be 'Execution terminated'. It was.

The manual reads well though.

Product	PC Logon version 2
Contact	RITS
Price	£95 with discounts for quantities
Good Points	Nice manual
Bad Points	Review copy did not work
Conclusions	A disappointment

RITS - Disk Lock Control version 2.0

Reviewed by John Silltow

This is a small utility product to provide disk control. This can just be disabling the floppy disks or incorporating full boot protection for the hard disk. It works only in the DOS environment and does not support dual boot, OS/2 or Novell systems.

A Master Disk is provided to set up the administration of this process and a Standard Installation Disk is provided which contains a subset of the running programs for use on all other users' machines.

Loading was through Windows although it is clearly a DOS based program that is called. However, it ran quickly and easily including adding an additional line in the CONFIG.SYS to invoke the protection and AUTOEXEC.BAT to repeat the call. Once loaded, the

PC needs to be re-booted for the changes to take effect. Strangely, the program does not tell you to do this.

Once having rebooted, the CONFIG.SYS and the program directory are automatically locked to prevent them being changed. At least that is what the manual said, unfortunately mine wasn't and I was able to read and edit files without hindrance.

The program itself worked well and prevented access to the floppy drives for read or write. The A: and B: icons were even removed from Windows File Manager.

In installing this program, I had used the Master Disk which provided various administration tools including the ability to create an authorisation diskette, a password to be stored on individual PCs or a challenge/response password system. All of these features are provided to enable various categories of user to access the floppy drives in the event of need. The diskettes are envisaged for engineers; the password can be used for remote support of a network machine and the challenge/response for distressed users being talked through a fix. I was not impressed that although loaded through Windows, no icon group was created to manage this. The program had to be run manually from Program Manager.

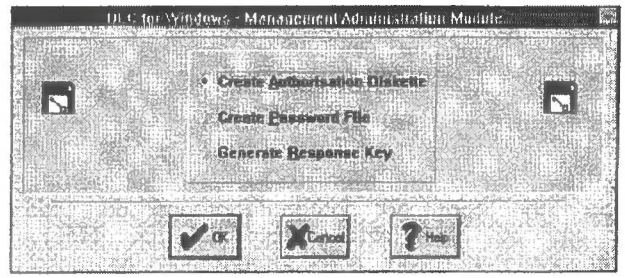
Having created an authorisation diskette I found this worked well and re-enabled the floppy drives (at least until next reboot) but again the program had to be manually called through Program Manager. As Windows itself is not continually refreshing, the fact the drives had been re-enabled was a complete mystery to it and its continued refusal to recognise them until itself rebooted should perhaps be commented on in the manual.

Although not as polished as it could be, this is a useful utility that, with some additional tweaking, could contribute to providing a secure environment.

Product	Drive Lock Control version 2
Contact	RITS 00 353 14973489
Price	£20 with discount for quantities
Good Points	Protection provided is good with various options for temporary removal.
Bad Points	Failed to protect CONFIG.SYS and no Windows icon.
Conclusions	Useful product as part of a secure environment.

RITS - Disk Lock Control version 2.0

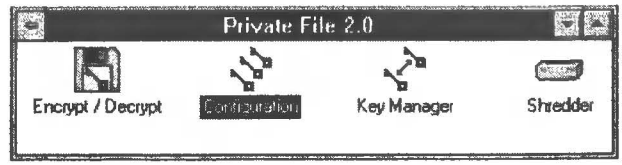
Management window to provide temporary disk drive access for various types of users such as Engineers, for remote support or distressed users requiring on-line help.



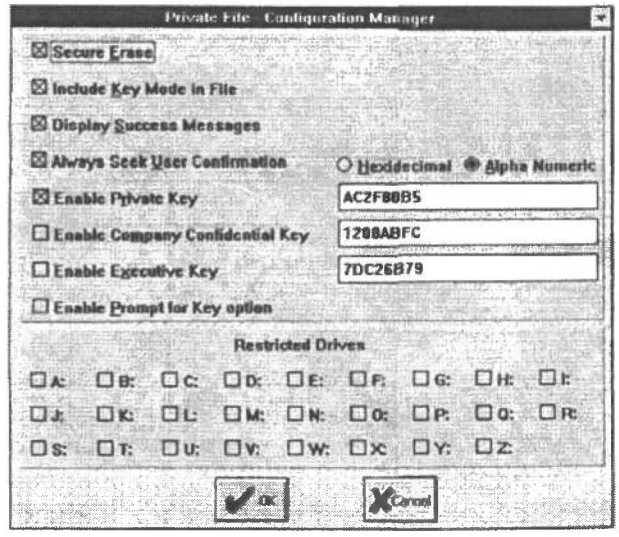
RTS - Private Review Version 2.0

Screen Shots

Basic Window showing the four options:



Encryption options showing the different ways it can be configured and the size and range of encryption keys available.



BOOK REVIEWS

This column is edited by Iltaph Khaliq who would like volunteers to help him with the review process. If you are interested please contact Iltaph on his number provided in the Editorial Panel.

TITLE: Internet Firewalls & Network Security

AUTHORS: Karanjit. S Siyan & Chris Hare

PUBLISHER: New Rider Publishing

ISBN: 1-56205-437-6

PRICE: £32.49

PAGES: 410 pages

REVIEWED BY: Iltaph Khaliq

The general criteria that I have used for book reviews in the past have been; Would I pay that kind of money for this book? and would it be useful on the office bookshelf?

I can report that I have done both with this book and as a result can feel honest about my comments on this review.

The Chapters are laid out as follows:

1) Understanding TCP/IP
2) Security
3) Designing a Network Policy
4) An Introduction to Screening Routers
5) Packet Filters
6) PC Packet Filtering
7) Firewall Architecture and Theory
8) Firewall Implementations

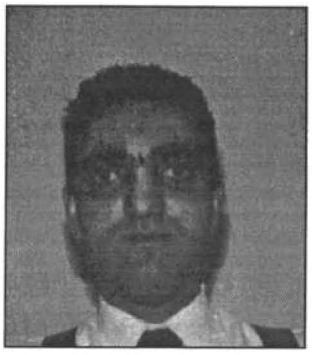
Appendices

Admission:

I fell asleep during Chapters 1 to 3, skipped straight to Chapters 7 and 8, skimmed through Chapters 4 to 6.

Within an hour of picking up the book, I'd grasped the problems and solutions. Within a day I'd agreed the necessary action with my Technical Support Group and within a week, we'd implemented our corporate Firewalls and laid out the Corporate policy.

The book is easy to use, well illustrated and has plenty for fanatics or bare essentials people alike. I found the illustrations particularly helpful. There are a large number of alternative Firewall structures illustrated and described within Chapter 7. At the same time, just about anything you might want to know about and around the subject is explained within the book, as the chapter layout and number of pages might suggest. I can recommend this book with hand on heart and it won't break the bank.



TITLE: Windows NT 3.5
Guidelines for Security, Audit and Control

AUTHORS: A joint research project by
Citibank N.A., Coopers & Lybrand,
The Institute of Internal Auditors and
Microsoft Corporation

PUBLISHER: Microsoft Press

ISBN: ISBN 1-55615-814-9

PRICE: £39.95

PAGES: 286 pages

REVIEWED BY: Iltaph Khaliq

The book is broken down into three main chapters and six appendices. On the whole it is a useful tool for auditors faced with the NT Operating System. To the experienced systems auditor, there will be many areas which appear to teach granny to suck eggs. The book would be invaluable to a general auditor within a small internal audit department, wishing to assure themselves of general controls and integrity operating overtheir network.

The Layout of the book is as follows:

Chapter 1:

Security Audit and Control Challenges (28 pages)

This provides a general outline of what a security policy is, why it is necessary and a suggested underlying infrastructure. It also provides an overview of the nature of systems auditing.

Chapter 2:

Windows NT, Audit and Control Features (136 pages)

This chapter claims that "Security in Windows NT was included as part of the initial design specifications".

The chapter outlines the key components of the security subsystem, being the Local Security Authority, the Security Account Manager and the Security Reference Monitor. It outlines the further security components, consisting of the Logon Process, Discretionary Access Controls, Access Tokens and Access Control Lists.

The descriptions are aided by illustrative diagrams and screenprints. Details are provided of the system's user account and profile security options, directory structuring, logon scripts and group compositions. There is a large amount of detailed explanation of the administration of the system, the security options available through file structuring, accompanying permissioning and allocation of ownership of directories and files.

There is a description of features within NT, aimed at assisting recovery in the event of a disaster. At the end of this chapter are 15 pages dedicated to features within NT designed to provide audit trails and these are :

Logon and Logoff, File and Object Access, Use of User Rights, User of Group Management, Security Policy Changes, Restart, Shutdown and System, and finally Process Tracking.

Each feature has an inactive default and therefore requires specific activation.

Chapter 3:

Auditing Windows NT (60 pages)

This chapter provides suggested audit objectives, procedures and tests based upon the previous contents of the book. These would undoubtedly provide a useful foundation for audit testing. Whilst the section comprises 60 pages, compilation of a test program would result in a substantially shorter schedule.

Appendices:

A) Baseline Security Standards

B) Advanced User ffights

C) Server Default Positions

D) Commands

E) Data Structures

F) Architecture

Final Comment:

It's all good stuff. Whilst there are plenty of compensating controls within the Operating System, I can't help feeling that with the degree of involvement from recognised auditing professionals, the issue of poor structuring and segregation of duties for Systems Administration with regard to the all powerful administration capabilities, should have been better catered for in both the product and the book.

"A RATHER UNLUCKY VESSEL"

The following letter appeared in the March edition of "Shipping World and Shipbuilder". Although not directly related to computer audit it does illustrate the 'Mitchell' law that problems occur not when one big thing goes wrong, but when many small things go wrong either simultaneously, or consecutively. The audit problem is trying to convince management, in advance, that such a string of coincidences may occur. You can always use this story to illustrate the point - Ed.

Dear Sir

It is with regret and haste that I write this letter to you, regret that such a small misunderstanding could lead to the following circumstances, and haste in order that you will get this report before you form your own preconceived opinions from reports in the press, for I am sure that they will tend to overdramatise the affair.

We had just picked up the pilot, and the apprentice had returned from changing the "G" flag for the "H" and, it being his first trip, was having difficulty in rolling the "G" flag up. I therefore proceeded to show him. Coming to the last part, I told him to "let go". The lad is willing but not too bright, necessitating my having to repeat the order in a sharper tone.

At this moment the Chief Officer appeared from the Chart Room, having been plotting the vessel's progress, and, thinking that it was the anchors that were being referred to, repeated the "let go" to the Third Officer on the forecastle. The port anchor having been cleared away but not walked out, was promptly let go. The effect of letting the anchor drop from the "pipe" while the vessel was proceeding at full harbour speed proved too much for the windlass brake, and the entire length of the port cable was pulled out "by the roots". I fear that the damage to the chain locker may be extensive. The braking effect of the port anchor naturally caused the vessel to sheer in that direction, towards the swing bridge that spans a tributary to the river we were navigating.

The swing bridge operator showed great presence of mind by opening the bridge for my vessel. Unfortunately, he did not think to stop the vehicular traffic, the result being that the bridge partly opened and deposited a Volkswagen, two cyclists, and a cattle truck on the foredeck. My ship's company are at present rounding up the contents of the latter, which from the noise I would say were pigs. In his efforts to stop the progress of the vessel, the Third Officer dropped the starboard anchor, too late to be of practical use, for it fell on the swing bridge operator's control cabin.

After the port anchor was let go and the vessel started to sheer, I gave a double ring Full Astern on the Engine Room Telegraph and personally rang the Engine Room to order maximum astern revolutions. I was informed that the sea temperature was 53°F and asked if there was a film tonight; my reply would not add constructively to this report.

Up to now I have confined my report to the activities at the forward end of the vessel. Down aft they were having their own problems. At the moment the port anchor was let go, the Second Officer was supervising the making fast of the after tug and was lowering the ship's towing spring down onto the tug.

The sudden braking effect on the port anchor caused the tug to "run in under" the stern of my vessel, just at the moment when the propeller was answering my double ring Full Astern. The prompt action of the Second Officer in securing the inboard end of the towing spring delayed the sinking of the tug by some minutes, thereby allowing the safe abandoning of that vessel.

It is strange, but at the very same moment of letting go the port anchor there was a power cut ashore. The fact that we were passing over a "cable area" at that time might suggest that we may have touched something on the river bed. It is perhaps lucky that the high-tension cables brought down by the foremast were not live, possibly being replaced by the underwater cable, but owing to the shore blackout it is impossible to say where the pylon fell.

It never fails to amaze me, the actions and behaviour of foreigners during moments of minor crisis. The pilot, for instance, is at the moment bundled in the corner of my day cabin, alternately crooning to himself and crying after having consumed a bottle of gin in a time that is worthy of inclusion in the Guinness Book of Records. The tug captain, on the other hand, reacted violently and had to forcibly be restrained by the Steward, who has him handcuffed in the ship's hospital, where he is telling me to do impossible things with my ship and my person.

I enclose the names and addresses of the drivers and insurance companies of the vehicles on my foredeck, which the Third Officer collected after his somewhat hurried evacuation of the forecastle. These particulars will enable you to claim for the damage that they did to the railings of the No. 1 hold.

I am closing this preliminary report, for I am finding it difficult to concentrate with the sound of police sirens and their flashing lights. It is sad to think that had the apprentice realised that there is no need to fly pilot flags after dark, none of this would have happened.

Yours etc.

A GLOBAL GAUGE OF GREASED PALMS

The following was recently published in the New York Times. It purports to rank the amount of corruption in 41 countries, calculated from surveys of businessmen and journalists. A ranking of 10 would be a place in which no corruption was found and 0 a place in which corruption was perceived to be everywhere. This may be useful to those of you who travel abroad - Ed.

Indonesia	1.94	Japan	6.72
China	2.16	Belgium/Luxembourg	6.85
Pakistan	2.25	France	7.00
Venezuela	2.66	Hong Kong	7.12
Brazil	2.70	Austria	7.13
Philippines	2.77	United States	7.79
India	2.78	Chile	7.94
Thailand	2.79	Germany	8.14
Italy	2.99	Britain	8.57
Mexico	3.18	Ireland	8.57
Colombia	3.44	Norway	8.61
Greece	4.04	The Netherlands	8.69
Turkey	4.10	Switzerland	8.76
Hungary	4.12	Australia	8.80
South Korea	4.29	Canada	8.87
Spain	4.35	Sweden	8.87
Taiwan	5.08	Finland	9.12
Argentina	5.24	Singapore	9.26
Malaysia	5.28	Denmark	9.32
Portugal	5.56	New Zealand	9.55
South Africa	5.62		

CASG MATTERS

REPORT FROM THE MONEY BOX

This column, the first in a regular series of columns dealing with the financial matters of CASG, is prepared by Bill Barton our Treasurer.

I have been asked to provide a summary of the financial position of the group. Although this can be a fairly dry subject I shall try my best to provide a brief summary of our current position. The main objective of the group from a financial perspective is to break even each year, balancing income from subscriptions and meetings with expenditure on meetings and the magazine.

Our financial year runs until 30 April each year. As we have not held any meetings for which a charge has been made so far this year, our only income has been from subscriptions. To the end of August we had received subscription income of approximately £2,000. This is balanced by expenditure of approximately £1,500 on membership and technical briefing leaflets and £1,500 on the Summer 1995 journal.

We have a healthy bank balance of approximately £27,000 which has been built up from an excess of revenue over expenditure over the years. It is intended to use this money on projects which are of benefit to the group, for example, on a possible research project on the status of computer audit in the United Kingdom. If you have suggestions on how this money could be purposefully used, please contact our Chairman.

MEMBERSHIP UPDATE

This column is edited by Jenny Broadbent our Membership Secretary. If you have any queries, or points, about membership matters, then please contact her at the address provided in the Management Committee list elsewhere in the Journal.

Let me begin by welcoming all our new members. 26 new members have joined since I took over as membership secretary and so I hope that you will forgive me for not mentioning you each by name. I am looking forward to the next technical briefing not just for its technical content but, also as an opportunity to meet some of our members.

When I took over as membership secretary, I looked to see who our members were. Now, no one working in computer audit can be ignorant of the extent to which organisations are becoming, or are already, critically reliant on IT. None the less, when I did look at the membership records I was astonished by the diversity. We have nearly 400 members, covering an enormous range of organisations.

I puzzled over how to pass on the information about the membership. Summarise it into categories? Produce long lists? The possibilities seemed endlessly dull. Prompted by our editor, (or was that dragooned?) I have arrived at a solution. I plan to extend the 'professional networking' offered by the technical briefing sessions by inviting members to contribute short profiles about themselves and their work to future issues of the journal. Even as I write these words my heart sinks, I know what my reaction would be if I picked up the journal and read that - 'good idea, hope she doesn't ask me!' Well, be warned, she probably will, unless you should decide to volunteer!

See you at the next meeting.

Jenny Broadbent

PS Can I put in a plea to those whose renewal notices have not yet reached the top of their 'action' pile to let me have their subscriptions as soon as possible please?

MEMBER PROFILES

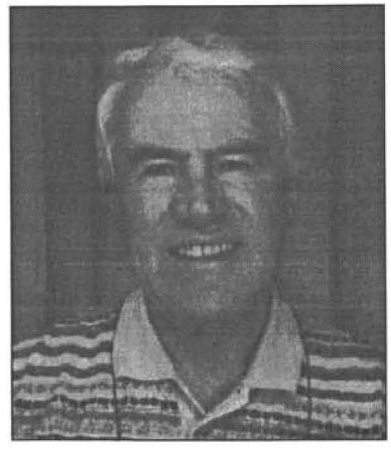
Edited by Jenny Broadbent

If you have a suggestion for someone to be profiled please contact Jenny at her number in the Editorial Panel

GEOFF WILSON

Current Position: Retired

CASG Involvement: Meetings Organiser



In so far as Information Systems are concerned, I could best be described as 'a poacher turned gamekeeper'. A systems analyst/programmer who defected to security!

In my younger days I had worked on a couple of farms, two banks, with a

couple of years National Service as a Gunner (mostly in Germany) and a further six in Ceylon, before becoming, in late 1956, a member of a team to specify, develop and implement the British Army's first computerised Pay system.

In mid 1963 I was given a first-hand opportunity to discover how well it worked by being posted to the pay team of an artillery regiment which then spent two and a half years in Malaysia. A further eighteen months in an Army Command headquarters elapsed before I returned to computing in the late summer of 1967.

The next ten plus years were divided between initially leading teams developing financial application programmes, and latterly, managing a group responsible for testing programmes and authorising their clearance for production. running.

In 1978, after almost 30 enjoyable years of Army life, I 'retired' and joined Cornhill Insurance's Information Systems department where I spent ten happy years in business systems development.

In 1988 I became their first Computer Security Manager (the penalty for an obsessive interest in 'controls' to prove accuracy and completeness of results?!). In the next five years I was actively involved in the development and implementation of the company security policy, its controls for user data access, and computer and business recovery planning. On reaching Cornhill's 'normal retirement age' of 63 I spent a further eighteen months with them on contract as a Consultant.

I joined the British Computer Society in 1962, and am currently a member of Hampshire Branch, because I believe that when you stop learning you start dying!

I'm also a grandfather, a churchwarden, and the local church treasurer.

JENNY BROADBENT

Current position: Computer audit manager - Cambridgeshire County Council

CASG involvement: Membership secretary

Jenny qualified with a small independent firm of Chartered Accountants in Chester before moving to Deloitte Haskins and Sells' Liverpool office. Now living in Cambridge, Jenny works part-time as computer audit manager for Cambridgeshire County Council and full time as a wife and mother. The move to computer audit came almost by accident and was not the most obvious career move for Jenny who had given up work in taxation early on because of the effort needed to keep up to date.....

Working for the Council, Jenny provides computer audit services not just to the County Council itself, but also to a number of other public service organisations within the county including District Councils, Addenbrookes hospital and Cambridgeshire Police Authority. In addition, Jenny manages the audit of the Council's key financial systems.

This provides an interesting and varied workload and an opportunity to work in organisations with cultures that vary widely. Most of her work centres on non-financial systems and, as a local, Jenny finds it easy to relate to the aims and objectives of the various organisations she audits (and hopes that the police soon track down the individuals who visited her house via the kitchen window while she was on holiday....).

Audits are fitted-in around a constant flurry of schools runs, forgotten PE kits and school plays. Balancing these various commitments requires precision planning and split second timing - both areas which Jenny finds particularly challenging! However, in the specialist area of crisis management Jenny comes into her own.

In her spare time Jenny is a loyal member of the Girton Ladies Book Group but, her main interest is gardening and the perennial battle with ground elder looms large in her life. In fact, a career change to landscape garden design looks increasingly attractive.....

BCS MATTERS

This is the second of a regular series of articles by Colin Thompson, the BCS Membership Director, which will focus mainly on BCS news and events. The aim will be to keep readers in touch with what is going on in the BCS. and to provide background information and explanation where appropriate. Anyone with suggestions for particular issues to be covered in future editions should contact Colin at BCS HQ

Tel: 01793 417410 e-mail: cthompson@bcs.org.uk).

PRIVY COUNCIL SUBMISSION

After a lengthy period of consultation with the Engineering Council, the submission for the amendment to the Royal Charter finally went to the Privy Council in May. The submission covers a number of proposed changes, including the creation of Graduate and Companion grades and the introduction of the title "Chartered Information Systems Practitioner" for Members and Fellows. The Privy Council will now consult a number of other bodies, including the Engineering Council - hence the need to clear any reservations there before making the submission - and a response is expected later in the year.

REINSTATEMENT CAMPAIGN

As part of the 1995/6 recruitment campaign, the Society is attempting to attract ex members back into membership. For a limited period the normal reinstatement charge (equivalent to one years subscription) has been waived and past members can now rejoin free of charge.

Anyone interested in reinstatement, or in assisting with the recruitment campaign itself, should contact the Membership Department at BCS HQ.

THE BCS YEARBOOK

The BCS yearbook, last published in 1989/90, reappeared this year under the title The BCS Review and Directory 1995. The book contains a full listing of all professional members of the Society together with more than 30 articles on issues of current interest within IS and over 20 pages of information on the Society itself. The Review and Directory is available to members at £10, including p&p and sales so far are approaching 5000.

BCS ANNUAL DINNER

Every year the British Computer Society Annual Dinner brings together some of the key IT professionals in the UK - managers, specialists, strategists, personalities and practitioners. Last year 400 people attended this event representing over 140 organisations, with 26 major companies sponsoring tables. This year the Dinner will be on 25th October, and will be held once again at the Park Lane Hotel in London, following the BCS Annual General Meeting.

The opportunity for those involved in the IT industry to meet and exchange views and experiences is what makes the BCS Annual Dinner such a success each year. It is also the occasion when the new BCS President makes his inaugural speech.

This year we are delighted to have Peter Moloney as the Guest Speaker. This highly entertaining former Trappist Monk, Officer in the Parachute Regiment, Missionary in West Africa and Teacher in Liverpool, has been awarded the prestigious title Benedictine After Dinner Speaker of the Year. (No I have never heard of it either, but I have heard Peter Moloney and he is a very entertaining speaker.)

The response to the toast to the guests will be given by Dr John Taylor, Director of Hewlett-Packard Laboratories Europe; and musical entertainment will be provided by the Paul Hodgson Quintet. Paul Hodgson's IMPROVISER music tutorial project won a medal in the 1994 BCS Annual Awards.

BCS AWARDS

The Oscars and the Booker Prize are rewards for excellence which also achieve extensive recognition from the general public. Although almost all professionals have their own system for honouring excellence, few capture the public imagination to the extent of those for film and fiction. This may be because most professions have a limited influence on the public at large.

Now Information Technology is playing an increasing part in everyone's lives, and this is reflected in the history of the British Computer Society Awards, which since the early 1970s have acted as both a mirror and a signpost to the future.

The BCS Awards Scheme aims to encourage the very best in UK Information technology and its applications. Normally three Awards are made each year, which are presented to projects that demonstrate excellence and the relevance or significance of computing.

The early Award winners were almost exclusively devoted to large mainframe based projects. But the Awards soon started to recognise the changes within the industry, with the result that many nominations and winners now run on PCs and workstations, and there has been a marked increase in the number of projects that directly affect the everyday lives of both the general public and industry.

The BCS awards are much more extensive than the Oscars, because they encompass not only excellence in computing, but also the widest possible range of social benefit and business valuc to society at large. Pride in our industry requires recognition of the technical and professional skills that flourish in the UK, and it is vital that the all embracing nature of IT across business and social spheres is realised.

In addition to the active endorsement of the Duke of Kent, the BCS in conjunction with the sponsors, is actively working towards achieving widespread recognition of the Awards, their importance, and their relevance to the community. In addition to the honour of winning, recognition brings with it the potential for increased publicity. Whether the work concerned is outstanding for its technical achievement, its imaginative use of Information Technology, or its wider benefit to society, acknowledgement of its status can only be advantageous.

Over their twenty three years the Awards have become established as the computer industry's most prestigious form of acknowledgement, a fact reflected by the major companies that are prepared to associate themselves with the Awards and by the recognition gained by the winners as a result of their success.

This year the BCS Awards are sponsored by BT, Bull, Computer People, DTI, Energis, Fraser Williams, Logica, IBM, ICL, The Post Office, Oracle and Tandem.

Award winners for 1994 were SuperJANET by Ukerna; PLATO-UK by the National Poisons Unit, Guy's and St Thomas' Hospital Trust and Royal Botanic Gardens, Kew; and The Read Codes by the NHS Centre for Coding and Classification.

The names of this year's winners will be announced on 29th November at an event to be held at the Waldorf Hotel in London. The ten medallists will demonstrate their projects through the day. Over lunch the three winners will be presented with their Awards by Lord Weinstock of GEC, and in the afternoon, the public are invited to come and see for themselves the winning projects.

For further information about the Awards or the Dinner please contact Anna Duckworth at BCS 01793 417433, email aduckworth@bcs.org.uk.

Library Services for BCS members

By Helen Crawford - BCS Librarian

The BCS library, which is held at the Institute for Electrical Engineers, is also available to members of BCS specialist groups. In this new column, Helen Crawford, the BCS Librarian, describes some of the facilities available. Future columns will discuss the many security and control publications held in the library.

Background

The BCS library has been housed at the Institution of Electrical Engineers (IEE) since 1977. The entire book collection exceeds 60,000 items, and periodicals amount to over 3,000 titles, some 1,100 currently taken.

Users of the library will find one of the largest collections of material in the fields of electrical and electronic engineering, manufacturing engineering, computing and information technology, control, communications and management. Books and journals on computing make up over 50% of the recent collection covering all areas of the subject. The areas are too numerous to list here but CASG members will be particularly interested in computer security. There is also an extensive collection of directories, dictionaries and other reference books.

Records of all items within the library are held on our in-house computer catalogue. Work is currently being undertaken to have this information available on the Internet.

Members of the BCS may take advantage of a range of library and information services:

Lending and Reference Services

Members may borrow up to ten books for a period of four weeks and may renew if the item is not required by another reader. A postal loans service is available free of charge.

Photocopy and Document Supply Services

Members may obtain, for a small charge, photocopies of articles from journals and conference proceedings under the terms of the copyright act. Items which are not in our stock can be obtained through inter-library loan.

Information Services

The library incorporates a technical and business information service. The information officers have access to over 1,000 of the world's major technical and business databases. BCS members desiring commercial, market and/or technical information may discuss their requirements with trained information officers and appropriate information sources will be consulted to provide customised answers to enquiries. Estimates of cost will be given in advance.

Courses Information Services

The courses information officer provides data on courses in higher and further education for continuing professional development.

Further information

The library and information services are available between 9 am and 5pm, Monday to Friday.

Further information about the library and its services may be obtained from:

The Library,
Institution of Electrical Engineers,
2 Savoy Place,
London,
WC2R 0BL.
Telephone 0171 344 5461,
Fax 0171 497 3557,
email libdesk@iee.org.uk

Estimating Software Development Time & Costs

George Allan

Abstract

This paper, which comprises three parts, aims to introduce and explain a process for software estimating. It is anticipated that this will provide auditors, software engineers and project managers with an insight to a stable method for estimating time, cost and staffing requirements. The basic model distinguishes between three different development modes - Organic, Semi-detached and Embedded. These are explained and worked examples are included to illustrate the theoretical points.

Further refinements to the model allow estimates to be made for more detailed partitioning of the development cycle. This paper discusses the time, cost and staffing requirements for Product Design, the actual Programming and the Integration & Testing of software units. A further consideration sub-divides the actual programming into its two realistic components of Detailed Design and Coding. Worked examples throughout are progressive in difficulty as each point is illustrated and accumulated into the auditor's/software engineer's/project manager's tool kit.

Key Words

Software estimating; CoCoMo; Person months; Development time; Development cost; Organic mode; Semi-detached mode; Embedded mode; Product design; Programming; Integration & Test; Detailed design; Code & unit test

Part 1 of 3

INTRODUCTION

The successful development of a modern day Information System (IS) which involves the writing of software units (sometimes referred to as modules) demands much more than a modern block structured programming language and a powerful operating system. There is a need for tools and toolsets to help with all aspects of system development not least of all aiding project management in software estimating and planning. No tool or model can remove the vital need for hard won experience but such models can aid and channel that experience in a positive direction.

The three questions that a planner or auditor needs to know about a prospective software unit are:-

- *How long will it take?*
- *How much will it cost?*
- *How many people will it need?*

A number of estimating models have emerged to provide the project managers with a selection of potentially useful tools. **The model discussed here specialises in DURATION, MANPOWER and COST** and was developed as the result of a research project based on previously gathered statistics of 63 software projects of varying sizes and complexities (Boehm 1981).

This is the *Constructive Cost Model* (CoCoMo) which is an algorithmic software estimation model. Algorithmic means that it is based on formulae derived by observing the above software developments. [Acknowledgement to research carried out by Dr Barry W Boehm]

This paper will describe the method of software estimation and introduce the concept of development mode. It will then explain the three basic development mode equations needed to estimate the cost of constructing a software unit. A number of worked examples are used to estimate the effort, work out the time, derive the number of programmers and calculate the costs for a variety of software units.

BASIC COCOMO FUNDAMENTALS

The fundamental concept is that *the amount of effort required in writing a software unit will depend of the size of that unit.* The relationship is not linear i.e. a unit twice as long does not require exactly twice the effort.

The general idea is that the EFFORT required by a team of programmers to write a software unit is measured in persons and months i.e. we say a unit will take 10 person months. This is 10 people all working for 1 month, or 2 people working for 5 months or 1 person working for 10 months etc. There are obvious limitations on this. For example if a unit requires 200 person months, it is impractical to have 1 person working for 200 months which is 16 years and 8 months, similarly there is an immense problem managing 200 people working for 1 month.

Effort

So we introduce the concept that the effort required is measured in person months. We stress that the units of measurement are persons times months and that we are estimating at this stage "manpower effort". This ***EFFORT*** is proportional to the ***SIZE*** of the software

unit measured in thousands of lines of code; each line representing one source instruction.

The generally accepted form is:

EFFORT is measured in Person Months = PM

SIZE is measured in = KDSI

Thousands (K) of Deliverable Source Instructions (KDSI).

Therefore the concept can be stated as

EFFORT (in Person Months) is proportional to MODULE SIZE in (KDSI)

$$PM \propto (KDSI)$$

The original research showed that the model requires the (KDSI) to be raised to a power and the whole of the right hand side to be multiplied by a coefficient. (see Table 1).

$$\therefore PM = A \times (KDSI)^B$$

This gives a first estimate of the manpower effort required to write a software module. We will see that the numbers A and B are provided to us depending on further information relating to with the complexity of the software itself. *The important step here is that once we know the size of the software unit and can find A & B, then we can calculate an estimate of person months of effort.* This will involve the use of a calculator, but we will keep the arithmetic as straight forward as possible.

Development Time

The next step is to estimate the Total Development Time. As this name implies, this is the time taken to develop a software unit from beginning to end. The Total Development time is known as TDEV and is usually measured in MONTHS. It may appear that once we have estimated the *EFFORT* as so-many-person-months, we could divide this figure by the number of programmers available and work out the time. As we saw before this has problems. So, taking a more scientific approach we say that:

Total Development time TDEV is based on Effort as follows:-

$$TDEV = 2.5 (PM)^C$$

where the power C is also given to us depending on the software module complexity.

The coefficient and powers A, B, C depend on the size and complexity of the software unit under consideration and also the environment in which that software is being developed. As we will see later A, B and C can all be looked up in reference tables.

Development Modes

There are three basic modes of development ranging from simplest to most complex with a middle ground. These have become known as:-

Simplest -Organic Mode

Middle Ground -Semi-Detached Mode

Most Complex -Embedded Mode

There are no crystal clear cut boundaries between these 3 modes of development and an experienced Project Manager will need to use his judgement when deciding which mode a new unit of software will fall into.

Let us say as a general rule the following:-

Type of Mode	**Type of Software Unit Under Construction**
ORGANIC MODE	Fairly simple construction, small KDSI, small team of programmers who all know the ropes.
SEMI-DETACHED MODE	The middle ground.
EMBEDDED MODE	Complex software, high KDSI upwards of 150 KDSI, large team with associated co-ordination problems.

Always remember that what we have here is only a starting point, giving BASIC estimates of Effort in PM and Duration in TDEV. The estimates are not refined in any way but are better than a pure guess at this early stage. These estimates may even be asked for at the very start of a project.

Worked Examples

As starting examples let us consider a small project developed in familiar surroundings where the programmers are familiar with the host machine and language; they know the physical procedures of the company and layout of the work area. This is the Organic mode in software development and the effort formula is:-

Effort requirement in person months = $PM = 2.4 \times (KDSI)^{1.05}$

That is to say $A = 2.4$

$B = 1.05$

Example 1

So for a software unit of size 8000 lines of instructions i.e. KDSI = 8

PM = 2.4 x (8)1.05 person months

= 2.4 x 8.88 person months

= 21.3 person months

The development time for the Organic mode software development is

TDEV = 2.5 x $(PM)^{0.38}$ months

So, in this case where PM = 21.3 person months

TDEV = 2.5 x $(21.3)^{0.38}$ months

= 2.5 x (3.2) months

= 8 months

CONCLUSION

A software unit of size 8 KDSI developed in Organic Mode will need 21.3 person months of effort and will take 8 months to develop.

Example 2

Consider another example where the size is 32,000 lines i.e. KDSI = 32.

So, Effort in person months

PM = 2.4 $(KDSI)^{1.05}$ person months

= 2.4 $(32)^{1.05}$ person months

= 2.4 (38.05) person months

= 91.3 person months

Development Time in months for Organic Mode is

TDEV = 2.5 $(PM)^{0.38}$ months

= 2.5 $(91.3)^{0.38}$ months

= 2.5 (5.56) months

= 13.9 months

CONCLUSION

A software unit of size 32 KDSI developed in Organic Mode will need 91.3 person months of Effort and will take 13.9 months to develop.

Now, from the above examples we could work out the average number of programmers required.

If we divide the EFFORT in person months by TDEV in months

$$\frac{\text{EFFORT in person months}}{\text{DEVELOPMENT TIME in months}} = \frac{\text{persons x months}}{\text{months}} = \text{persons}$$

So for example 1 we have:-

$$\frac{PM}{TDEV} = \frac{21.3}{8} \text{ persons} = \text{just over } 2\frac{1}{2} \text{ persons}$$

For example 2

$$\frac{PM}{TDEV} = \frac{91.3}{13.9} \text{ persons} = \text{just over } 6\frac{1}{2} \text{ persons}$$

This is the way to estimate the programmer requirements in software development.

To recap so far, if we know the size of a software module in KDSI - thousands of deliverable source instructions - we can estimate the EFFORT in PERSON MONTHS.

EFFORT = PM = 2.4 x $(KDSI)^{1.05}$ Person Months

From this estimate of EFFORT we can estimate the Total Development Time TDEV in MONTHS.

TDEV = 2.5 x $(PM)^{0.38}$

From EFFORT in Person Months and TDEV in months we can estimate the average staff required.

$$\text{Average Staff Requirement} = \frac{PM}{TDEV}$$

THE DEVELOPMENT MODES

Let us now say more about the three different development modes.

- Organic
- Semi-Detached
- Embedded

These represent progressively more hostile development environments. When developing software units there are a ***number of factors that help or hinder*** the programmers in their work. Some of the more obvious of these are:-

- Extent of knowledge of the programming language being used.
- Complexity of software.
- Size of module.
- Familiarity with the host computer system and operating system.
- How the team hold together and work together.
- Management practices & testing routines.
- Working practices & office routines.

When all the factors are considered together this gives us an idea of the work conditions under which this software unit is being developed. This is known as the DEVELOPMENT MODE.

Organic Mode

This is usually a fairly stable environment where work is in a small software team who all know each other's capabilities. The hardware and operating system will be familiar and not require constant upgrading and development which would hinder software development. The software unit will not normally be more than 50 KDSI.

The software team are all likely to be permanent members of staff familiar with the in-house environment, domestic routine and company policy. They will all be experienced in the type of system for which this new unit is being developed. This has great advantages not only in developing/writing the new code but also in the testing procedures. There should not be any need to contract new staff who need training in the host system, language to be used or other aspects of the company that may delay the immediate participation in an active role in productive software development. This should all lead to a familiarity with one's fellow workers and friendly working practices leading to a relaxed and productive atmosphere. Software development is likely to be a smooth process following design without strict and stringent rules and regulations between processes which would inhibit development.

Communication between Analyst/Designer and Programmer should be well established and queries will be sorted out quickly and effectively without recourse to large amounts of bureaucratic paperwork.

Examples of Software Units Developed in Organic Mode

- A new unit developed in-house to fit into an already well established project.
- A new stock control system written by the well established in-house software cell.
- A small and straight forward new unit without any hidden snags.

Embedded Mode

This typifies the very large and complicated software module which is itself just one module in a very large and complex project. The module will be upwards of 150 KDSI and this may be further complicated by the target system being new and unfamiliar to the programmer. Certain parts of the new system will probably cover new and innovative ground and be unfamiliar to the programmers. Therefore the development will need a tightly constrained system of controls and monitoring points to ensure compliance with the original requirements, the technical and interface specifications.

Being large and complex, this software development will require careful communication procedures if the module is to be successful in the overall project as well as each unit development within the module. Having a large number of programmers and testers at a variety of levels and grades may of necessity require a further level of management with its inherent problems. This in itself may require more staff than are currently available within the present company - so new staff will be recruited and they will require time to settle in. They will also need training before being competent and contribute effectively to the software development in hand.

Examples of Software Units developed in Embedded Mode

- An aircraft flight simulator :
- Traffic light control system for a large city.
- The total software for a large nuclear power station.

Semi-Detached Mode

The Semi-Detached development mode represents the middle-way between Organic and Embedded. This is likely to be a module of less than 300 KDSI where the team members have some experience of related systems and moderate experience of the development aids to hand. This could be a mix of some new members and some established programmers, or possibly most of the existing team with an intermediate level of expertise. The module will require a reasonable amount of monitoring and control to ensure adherence to specification and interfaces but also should allow a degree of on-site communication to interpret the original requirements and clarify points of difficulty.

Examples of Software Units developed in Semi-Detached Mode

- A training simulator for Point-of-Sales.
- On-line real-time finger print recognition system cross referencing criminal records.
- Fuel and store for ocean going freight carriers.
- A resource scheduler with a large number of interdependent parameters to consider.

For systems with such varied characteristics it will be no surprise to learn that the coefficients and powers in the pair of equations representing effort requirement and development time will be different in each of the three. So, for each of the development modes we can state the following two basic equations:-

BASIC CoCoMo TABLE

Basic Development Mode Equations

Organic

PM = 2.4(KDSI) 1.05 TDEV = 2.5(PM) 0.38

Semi-Detached

PM = 3.0(KDSI) 1.12 TDEV = 2.5(PM) 0.35

Embedded

PM = 3.6(KDSI) 1.20 TDEV = 2.5(PM) 0.32

Table 1 : Effort & TDEV

Worked Examples

Example 3

Consider a Semi-Detached Mode unit with an expected size of 20 KDSI.

Required effort
in person months
= PM = 3.0 x $(KDSI)^{1.12}$ person months of effort

= 3.0 x $(20)^{1.12}$ person months of effort

= 3 0 x 28.65 person months of effort

= 85.96 person months of effort

Development time
in months
= TDEV = 2.5 x $(PM)^{0.35}$ months

= 2.5 x $(86)^{0.35}$ months

= 2.5 x 4.75 months

= 11.9 months

CONCLUSION

A Software Unit developed of size 20 KDSI developed in Semi-Detached Mode will require 86 Person Months of Effort and take 12 months to develop.

Notice the rounding. This has to be sensible and we advocate a maximum of 1 decimal place - more defeats the object of the estimate - less makes the estimate unsound and unreliable.

Example 4 Consider an Embedded mode unit of size 320 KDSI.

So, for Embedded Mode

Required effort in
person months
= PM = 3.6 x $(KDSI)^{1.20}$ person months of effort

= 3.6 x $(320)^{1.20}$ person months of effort

= 3.6 x 1014.3 person months of effort

= 3651.6 person months of effort

Duration
= TDEV = 2.5 x $(PM)^{0.32}$ months

= 2.5 x $(3651.6)^{0.32}$ months

= 2.5 x 13.8 months

= 34.5 months

Conclusion

The Embedded Mode Software Unit of size 320 KDSI is estimated to need 3652 Person Months of Effort and take 34.5 months development time.

Cost

Finally in this section, let us take our first look at how much a software unit will cost.

We now have a rough idea of the average number of staff required and the time in months this number of people will be working. If we coupled this with the cost per month of the average staff member we would have a first estimate of staff development costs.

Average Number of Staff x Development Time in Months x Cost per Programmer per Month.

The Reader should notice that Average Number of Staff was obtained from:

$$\text{Average Number of Staff} = \frac{PM}{TDEV}$$

So, Average Number of Staff x Development Time

$$= \frac{PM}{TDEV} \times TDEV = PM$$

In other words

Staff Costs = PM x Cost per Programmer per Month

This is sensible when we think that PM = Persons x Months and when this is multiplied by Cost per Person per Month this will give the Cost of the software unit.

So, if we couple the development EFFORT with the monthly cost of a programmer we could estimate the total cost of this software unit.

The number of person months of EFFORT x Cost per person per month = Total cost estimate for a unit of this size.

Worked Examples

If the average cost of a programmer to the company is £2000 per month,

then in Example 1 the estimated cost of the software module =

PM x monthly cost = 21.3 x £2000 = £42,600

in Example 2

Estimated cost = 91.3 x £2000 = £182,600

SUMMARY SO FAR

So far we have calculated estimates for Effort, overall Development Time and Cost based on average staff. The steps in order are:-

1. Calculate manpower effort in person months PM.
2. Calculate total development time TDEV in months.
3. Derive the average number of staff required by dividing PM by TDEV.
4. Calculate overall average cost by taking the effort in person months (PM) multiplied by cost of each person per month.

NB

Important points to observe at this stage are:-

I. All the above are only to be regarded as basic estimates based on initial information available very early on in the project. These estimates could even be asked for at the tendering stage for pricing the contract.

II. The estimates all depend on ONLY ONE PARAMETER namely the software size in KDSI.

III. This software size has been given to us by a third party, or may be "guestimated" based on little else than someone's "feel for the problem".

DO NOT LOOSE SIGHT OF THESE IMPORTANT POINTS.

We have known instances where these initial estimates have been taken as tablets of stone and eventually been written into contractually binding documents leading to horrendous problems for the Project Manager, Team Leaders and Senior Programmers.

DON'T LET MILESTONES BECOME MILLSTONES

REFERENCE

Boehm B (1981) Software Engineering Economics, Prentice-Hall

End of Part One of Three - To be continued in the next edition

The Author

George Allan is a Senior Lecturer in the Department of Information Science at Portsmouth University and the Academic Editor for this Journal. He will be 'profiled' in the next edition, but if you wish to contact him in the interim please see the contact details provided under the Editorial Panel.

British
Computer
Society

PLEASE RETURN TO
Jenny Broadbent
CASG Membership Secretary
Room C309
Cambridgeshire County Council
Shire Hall
Castle Hill
Cambridge CB3 0AP

Membership Application

(Membership runs from June to the following May 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)* £75

* Corporate members may nominate up to 4 additional recipients for direct mailing of the Journal and attendance at our meetings *(see over)*

INDIVIDUAL MEMBERSHIP *(NOT a member of the BCS)* £25

INDIVIDUAL MEMBERSHIP *(A members of the BCS)* £15

BCS membership number: _____

STUDENT MEMBERSHIP (Full-time only and must be supported by a letter from the educational establishment).

Educational Establishment: _____ £10

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

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

PLEASE MAKE CHEQUES PAYABLE TO "BCS CASG"
AND RETURN WITH THIS FORM TO THE ADDRESS SHOWN ABOVE

ADDITIONAL CORPORATE MEMBERS

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:

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

INDIVIDUAL NAME:
(Title/Initials/Surname)

POSITION:

ORGANISATION:

ADDRESS:

POST CODE:

TELEPHONE: (STD Code/Number/Extension)

PROFESSIONAL CATEGORY:

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

British
Computer
Society

Management Committee

CHAIRMAN	Alison Webb	Independent Consultant	01223 461316
SECRETARY	Raghu Iyer	KPMG	0171 311 6023
		Email: raghu.iyer@kpmg.mark400.gb	
TREASURER	Bill Barton	B Sky B	0171 705 6821
MEMBERSHIP SECRETARY	Jenny Broadbent	Cambridgeshire County Council	01223 317256
JOURNAL EDITOR	John Mitchell	LHS - The Business Control Consultancy	01707 851454
		Email: jmitchell@lhs.win-uk.net	
MEETINGS	Paul Howitt	Tesco Stores Limited	01992 644250
	Jim Ewers	Hertfordshire County Council	01992 555328
	John Bevan	Audit &Computer Security Services	01992 582439
	Geoff Wilson	Independent Consultant	01962 733049
	Allen Brown	Independent Consultant	01803 327874
	Diane Skinner	Audit Commission	01179 236757

Membership Enquiries to:

Jenny Broadbent
Room C309
Cambridgeshire County Council
Shire Hall
Castle Hill
Cambridge
CB3 0AP

Tel: 01223 317256

casg
Computer Audit Specialist Group

Presents

Information Highways:

The Opportunities for Good and Ill

Tuesday 16 January 1996
9.30 am for 10.00 am at
The Royal Aeronautical Society,
4 Hamilton Place, London W1V 0BQ

British Computer Society

The second of our full-day technical briefings. This one reflects on the opportunities for good and ill which currently exist both on the internet and on more local routes! It includes the expanding role of the "traffic policeman", as the day also considers the audit and security issues surrounding electronic mail and telephone systems.

This is an unrepeatable and very affordable chance to see a demonstration of E-Mail and the World Wide Web, and to hear from top-class speakers and fellow professionals about aspects of communication which we ALL may now need to consider in our everyday working and leisure lives.

Registration Procedure

The fee for the day, which includes conference papers, coffee, lunch and tea is £40.00 (net of VAT; gross £47.00) for members of the following organisations:-

BCS, CASG, CIPFA, ISACA, ICAEW IT Faculty

The fee for non-members is £140.00 (net of VAT; gross £164.50)

A Registration Form is enclosed with this issue of the Journal. The non-member fee includes the cost of Corporate Membership of the Computer Audit Specialist Group for the season 1995/96, so please complete the membership form on the back of the Registration Form.

Individual non-members will be accepted at the member rate if they also enrol as CASG members at the same time, using the membership application form on the reverse of the Registration Form.

Venue for Technical Briefings

Royal Aeronautical Society,
4 Hamilton Place
London W1V 0BQ