TOPIC: EFFECTIVE INFORMATION SECURITY DOCUMENTS

ABSTRACT: This paper examines the principles underlying the production of effective and useful information security documents, fit for purpose, and efficient in their consumption of effort. These principles are being implemented in the next release of Information Security Memorandum 5, the standard for the production of Security Policies for United Kingdom military and government civilian organisations and for government contractors. The author is currently rewriting this Memorandum.

AUTHOR: Michael E J Stubbings MBCS

AFFILIATION: Information Security Policy branch, Communications-Electronics Security Group, Cheltenham, United Kingdom

ADDRESS: Communications-Electronics Security Group,
Room 2/0503,
P.O. Box 144,
CHELTENHAM
Gloucestershire
GL52 5UE
United Kingdom

VOICE: +44-1242-221492 ext 4035

FAX: +44-1242-256482

EMAIL: mike_stubbings@cesg.gov.uk

SECURITY DOCUMENTS: WRITING THEM AND READING THEM

Introduction

We've all seen them: System Security Policies or Plans (SSPs) which are dense, turgid, undoubtedly accurate, and full of the minutiae of information security and configuration control. We've all seen the opposite too: documents so brief or superficial that we wonder why anyone bothered in the first place. Both approaches waste the time of writers and readers. Both approaches are ultimately detrimental to the effective discharge of information security responsibilities. Naturally, this also implies that business effectiveness has been compromised. What guidance can we give to those navigating their way between Scylla and Charybdis: between too much and not enough?

The Basics

The existence of a document has to be justified. If it can't be justified then writing it and reading it are a waste of time. Saying 'we always produce an SSP like this' is not a justification. Neither is 'the rules say that we must produce an SSP like this'. I realise that it is often easier and quicker to follow the rules than to challenge them, but rules that have outlived their usefulness usually stay in place until disputed by someone. At this point, I shall stop talking about SSPs and start talking about SPs - Security Policies. As noted later in this paper I'm not convinced that the 'system' is necessarily the most useful basis for information security documents.

What constitutes a justification for the existence of a document? I suggest that a justified document has the following characteristics:

1. It contains information not readily accessible elsewhere;
2. All of its information is needed by its target readership in order to do their jobs;
3. All of its information is presented in a form and manner readily accessible to its target readership;
4. When acted upon, the business interests of the commissioning organisation are advanced to a degree justifying the amount of effort used to produce the document;
5. It has defined conditions of validity - describing a past state of affairs, possessing a period of validity, or with clear document maintenance responsibilities.

Obviously, these principles could apply equally well to virtually any document. In the context of information security it must be remembered that the writers and readers of SPs, for example, are expensive, and often over-worked, people. A waste of their time is a waste of money.

Another way of looking at this is to say that the writer must identify:

6. Purpose;
7. Content;
8. Readership;
9. Responsibility and Lifecycle;
10. Presentation.

Purpose

No-one at this Conference will need to be told that information security requirements and responsibilities vary enormously during the project lifecycle. Yet we often assume that one document, usually a Security Policy (SP), will be able to function like a Swiss Army penknife: useful for any purpose under the sun. I shall consider briefly some of the purposes for which we write

information security documents, asking in each case whether we are right to do so.

Legal/Regulatory

Notwithstanding what I said earlier about obsolete rules, if the law or internal procedures dictate a particular type of document, it is likely that one is going simply to have to grit one's teeth and get on with it. But if the rules (particularly internal rules) mandate something which obviously does not add value to the organisation, this needs to pointed out. For example, SP formats which list all the hardware and software in an office environment mean extra work every time any form of upgrade takes place or a piece of kit is moved. If there is a good Configuration Control Board (CCB) in existence, keeping adequate records, why bother with the list in the SP? The CCB's list is all that is needed.

Feasibility Studies

When a project proposal is submitted, I suggest that a separate security document could be counter-productive. This is for two reasons: one philosophical, and the other practical. The philosophical reason is that a project proposal is about satisfying business objectives. It's not primarily about technology; it's about business, and everything in it should be orientated towards achieving a defined set of business objectives. Information Security is one of those objectives, and has always to be viewed and expressed primarily in business terms. Our profession is about adding value to the products or services provided by our employers, or at the very least preventing value being lost. The costs of a particular information security profile can then be seen in the context of what that profile accomplishes in business terms. If security is defined separately then it is likely to be seen as an external factor, or as a hurdle, bearing no relationship to the 'real' work of providing some new facility. So, get information security in there as a business objective along with all the other business objectives, right from the start. And the practical reason? The fewer separate documents we have to write, review and read, the better.

In summary:
Purpose: Investment decision guidance
Vocabulary: Business-orientated
Readership: Investment decision makers

Procurement

This is a difficult subject, covering a wide range of contractual arrangements and specifications. In the United Kingdom, we have PFI - the Private Finance Initiative, whereby government invites companies both to invest in government work and to take responsibility for some of the concomitant financial risks. Under this system government submits a specification of the services it requires, rather than the products. It's up to the service supplier to work out how best to satisfy the requirement. There are obvious parallels with outsourcing and facilities management, and the setting up of Service Level Agreements (SLAs). Infosec professionals should review both the Invitations To Tender (ITTs) and the submissions by prospective suppliers. At this level, it is unreasonable to expect security requirements to be expressed in anything but business terms. The service supplier may for example choose to submit a system high solution with a stand-alone element for sensitive material, or a multi-level solution. We might define in high level terms the types of event we want audited, but we will not specify how audit records are to be organised or stored. It is the service which gets specified in an ITT, not an outline solution. In the case of a facilities management ITT, we are likely to specify, for example, the response time for reporting suspected security breaches. We would not set out how they would organise themselves and their records to achieve this. As with Feasibility Studies, the intended readership contains groups of people interested primarily in business decisions,

or at least in management issues. It is their needs and their vocabulary which should regulate how we express ourselves, and what we say.

We should still, therefore, be talking about security in terms of business objectives. If the security services required from the contractor are sufficiently complex, we might want a separate document. If so, it must be within the document hierarchy describing other aspects of the service; it must not be some separate set of rules defined in terms unrelated to the immediate business objectives. What we are discussing is most definitely not an SP. It is a business service specification, and must be looked at in entirely functional terms. I'm not aware that we have templates for this sort of requirement, or even whether templates are practical. If we know our businesses, I have no doubt that we can produce what is required. In my own country I know of research being conducted into the notation of required security services.

There is still the classical project to acquire a product rather than a service. If the product is to be accredited as a unit, then an outline SP may well be the best approach. But beware of putting in too much detail. It only needs enough information to specify the security context (intended environment, legal/regulatory constraints, etc.). It's up to the contractor to sort out ways of accommodating this context. The context must still be tied to business objectives. Whether one does this in an outline SP or in another document is a matter for the writer's judgement.

In summary:
Purpose: Specification of service or product
Vocabulary: Orientated towards business or management
Readership: Potential provider or investment decision maker

Evaluation

I'm not familiar with the requirements of the USA's TCSEC system, but I am aware of the 'Security Target' requirements for the European ITSEC scheme, administered from within my own organisation, CESG. ITSEC publications set out clearly what the supporting documents should contain. A key part of the requirements is the SP. Evaluation is not my specialism, and I'm not going to comment on its documentary requirements. I will, however, raise a question for you to consider: Is the document set needed for the successful conduct of an evaluation necessarily appropriate to any of the other purposes discussed in this paper?

There are two reasons for asking this question. First of all, any system being evaluated is also going to need documents to meet some of these other purposes. Evaluation is likely to need the most technically detailed document set of any of them, and is likely to be conducted without the sort of direct relationship to business objectives which I have advocated elsewhere, being orientated rather towards specific technical objectives. I am aware that the Common Criteria approach may well change this, and that further development in this area can be expected. But at the moment, an evaluation document set is likely to be way over the top for other purposes and readerships, and may thus cause obfuscation rather than enlightenment. The second reason for asking the question is that most systems being accredited to hold protectively marked (i.e. classified) material are never going to be evaluated. Under these circumstances there is no point whatsoever in constructing a document set according to templates designed for evaluation. This principle is recognised in rewriting CESG's Information Security Memorandum Number 5.

In summary:
Purpose: Specification of evaluation target
Vocabulary: Technical
Readership: Evaluators

Operation

The role of the SP in operational security documents has traditionally been as the point of ultimate reference for all measures mandated for operational use. It should be possible to identify each security instruction as a counter-measure to a particular threat stated in the SP. That's the theory. It's certainly true that one should respect the maxim 'If it doesn't buy you anything, don't do it'. And it should certainly be possible to demonstrate that any operational measure (for example, enforcing an extra sign-on sequence) does buy you something of sufficient value to justify the financial and operational costs. These are fine principles, and one should pay attention to them. I would, however, counsel caution. Establishing such clear and comprehensive lines of derivation through a document set is itself a cost - in the writer's time, and in the time of anyone charged with maintaining the documents. Do as much as you need to in order to establish the wisdom of your provisions, but no more. More than enough is too much.

Operational security documents must be carefully directed towards particular groups of readers. There is no point in telling end-users about the way new accounts should be installed, or audit trails managed; it will only give them ideas, and in any case, the more irrelevant material is contained within a document, the more likely it is that the relevant stuff will be overlooked. I suggest that there are up to 4 different categories of operational document to be considered: System management; End user; Configuration Control; and Continuity Planning. The last one is an odd one out, so I will look at that first.

This is the one operational document which we hope will not get used in anger. It is also the one we as Infosec professionals are unlikely to write. Business Continuity Planning as an activity belongs to the enterprise rather than to individual systems. The priority of a particular system (or, more likely, a particular business activity) is not generally ours to specify. It may change according, for example, to the position in a yearly budgeting cycle. We will contribute to the writing, maintenance, and exercise of the Business Continuity Plan, and in some companies the whole thing may be our responsibility. I suggest, however, that this is such a particular requirement, that the whole disaster recovery scenario be viewed as a new situation, needing separate information security provisions and documents from those covering normal running. Don't worry overmuch (or even worry at all) about tie-ins with SPs or day-to-day operational security documents. If you end up using your Business Continuity Plan, neat tie-ins to your SPs will be the last thing on your mind.

The other 3 documents are simply workings out of certain basic principles. Some organisations put them all into one. This is only justified if the readership overlaps to such an extent that separation causes more problems than it solves. The principles are:

a) Tell people only what they need to know to do their jobs;
b) Use the terminology and concepts of the readership;
c) Keep the volume to a minimum;
d) Only specify measures which actually achieve something useful (satisfying an arbitrary rule doesn't count).

It is worth noting that sensible operational security measures are quite likely to be sensible from a performance management perspective also. For example, configuring routers for optimum performance will also involve preventing broadcast storms, with their associated denial of service potential. Where there is overlap - use it. There is a lot to be said for inserting security measures into the normal operational guidance provided for a system - it is after all just another way of contributing towards effective management and use. Separate documents for security should be avoided unless the benefits are obvious.

In summary:
Purpose: Operational guidance
Vocabulary: Terminology of the individual category of user
Readership: Various categories of user (e.g. system managers; end users)

Accreditation

I'm using this term in the classical government sense: the activity by which an authorised person formally accepts, on behalf of the organisation, the residual risks associated with running a particular set of IT resources in a particular manner. That person or group of people needs not only the material on which to base his or her decision, but also sufficient information to be able to justify the decision. The accreditor, after all, must be accountable. While we at CESG are publishing national guidance to accreditors about the compilation and documenting of information security requirements, it is our clear perception that for accountability to mean anything, we must allow accreditors the authority to specify for themselves what they require in their own local circumstances. For that reason, Memorandum 5 will mandate neither the contents nor the format of security policy documents. But the accreditors are accountable, and their decisions must be well founded.

In summary:
Purpose: Risk assessment and management summary
Vocabulary: Business/technical
Readership: Accreditors and data/process owners

Purpose - Conclusion

A document resembling a Swiss Army penknife (multi-purpose) is unlikely to be effective. The different readerships, purposes and vocabularies make it unlikely that even a gifted writer is going to be able to write a single document to meet all or even most of these requirements for anything but the most basic of IT resources. The attempt to do so is likely to be counter-productive, in that the difficulty of using a document for its intended purpose, more than negates any savings made by not writing a more targeted document set. I would in any case dispute that savings are necessarily made by producing very general documents. The true cost of any document involves its usability as well as the time it takes to write it, and targeted documents are more usable than more general examples, where one has to hunt through irrelevant material for the information one actually needs, and then struggle to understand it. In my experience, two short, well-targeted, documents are a good deal easier and quicker to write than one longer, more general, version.

Content

I have already said a good deal about content, in emphasising that documents must be orientated towards the needs and vocabulary of their readers. There are just two extra points that I would make: boundaries, and context.

Boundaries

In any one document, what are we describing? The answer is usually 'the system'; after all, we have long written System Security Policies (or Plans). Government approaches on both sides of the Atlantic - and elsewhere - have traditionally been shaped to fit monolithic systems: installed, accredited and used as a single entity. We have tweaked our standards to recognise the extensive networking which is now pervasive. I suggest that the time has come for us to consider other ways of setting our boundaries.
We have in fact already discussed this, in the Procurement and Business Continuity Planning sections

above, where the boundaries surround services or business functions, possibly crossing a number of technical boundaries. Accreditors and evaluators are now being sent Community Security Policies (CSPs), Network Security Policies (NSPs), and Application Security Policies (ASPs) - to say nothing of Programme Security Policies (PSPs) and business function security policies. So, flexibility of thinking is coming in. The main point here is that we should not automatically assume that a particular set of hardware is necessarily the best unit to be described in our security documents. My gut feeling is that in future, we are going to be much more concerned about the management domain than about a particular collection of boxes with flashing lights. I don't mean NT-type domains; I mean the resources managed by a particular group of people operating under one set of management procedures, or even under one manager. Within the Government Communications Headquarters (GCHQ, the parent department of my own group), the management domain is the prime unit of Infosec audit and monitoring. Some UK government organisations are making it the unit of accreditation as well, on the grounds that it is within a single team that a security approach is defined and implemented, both in its technical and non-technical aspects.

If you do choose non-system boundaries for your documents, it will be necessary to pay particular attention to interfaces. The classic SP has sections for 'interconnections', where one lists the systems to which one will permit connections. Any other boundary will also have its 'crossing places'. For example, an application's security profile may depend upon authentication services provided by the Common Operating Environment (COE). The COE's security profile may depend upon the protection given to the routers and bridges provided by the infrastructure management procedures. I know a UK accreditor who has adopted this approach, accrediting applications, COE and infrastructure separately, on the grounds that these were the real management domains, with 3 different sets of people, and these were where the security measures were applied. He thus avoided taking a vertical slice through the applications, workstations, servers, operating systems and network. This accreditor likened the resulting accreditation structure to the OSI 7-layer stack, where one has separate levels for different functions (Transport, Network, Applications etc.), and defines them largely in terms of controlled interfaces between adjacent layers. Once one has done that, there is a great deal of freedom in how one approaches what happens purely within any one level in the stack.

So, be flexible and imaginative. Choose your boundaries with care, selecting ones which are relevant to the way people and IT resources are organised. This can make it easier to write the documents, as one can avoid trying to specify measures in terms appropriate to very disparate groups of people.

Context

I spent nearly 4 years as an accreditor, before I moved into Infosec policy. In that time I have seen a constant leaning towards information security documents which concentrate on electronic measures at the expense of anything else. Years ago, I was a system and network manager, writing SSPs to get my systems accredited. I suspect that I did the same thing, and I also suspect that accreditors have, either by intention or by default, allowed this situation to continue. It is not healthy. I have already pointed out several times the relevance of business-orientated vocabulary, and the integration of information security objectives into the wider business objectives for the IT resources in question. This is focused most clearly in the requirements for procurement or Business Continuity Planning. IT resources have a context, and the primary aspect of that context is what the people using the resources want to do with them. Tell a user that they must use a password of at least 6 characters in length, not spelling a dictionary word forwards or backwards, if you must. But don't just give an instruction. When we were children we didn't like an adult saying 'Do this because I say so', and we don't win friends by doing so now. To say 'Do this, because if you don't you substantially increase the chance of someone else reading your e-mail' is entirely different. It's now in a business context, expressed in terms of what people actually want to do.

It's not simply a question of business context for electronic measures. We are familiar enough with procedural, physical and personnel security considerations, and these also have a business, or at least a cultural, context. Non-technical considerations, much more than technical ones, are closely related to the organisation's sense of identity. For example, a small business unit may pride itself on its cohesiveness, and on the way everyone knows everyone else. The introduction of photographic passes, and the checking of passes, might be resisted on cultural grounds (whether or not they actually *do* know each other that well). This is not to say that passes should not be introduced under such circumstances, but that the person designing and documenting the security profile for IT resources must be aware that everything has a human and a business context.

Readership

This subject has already been addressed sufficiently in this paper, particularly under the heading of Purpose. For the sake of emphasis, I will say again that a good document is well targeted, and meant to be used: not just read, but used. And if that's going to be done effectively, then the writer has to understand the readers: what they want, their priorities, and how they express themselves. Try to satisfy too many different groups, and one ends up satisfying no-one.

Responsibility and Lifecycle

The writer is responsible for the document - for a while. Some documents are static: minutes of meetings, briefing papers etc. They are only ever intended to describe the situation at a particular point in time. The question of continuing responsibility for such a document does not therefore arise. But IT resources are different. No-one reading this is likely to need telling that IT systems evolve, that the organisational structures in which they are set also change, that operational circumstances change, business requirements change, and that threats change. The static model is therefore inappropriate for documents to be used over the whole life of IT resources.

This fact of life has a number of consequences for the person planning and writing an information security document set. Some of these considerations overlap with ones already discussed under other headings. For example, if user guidance documents are divided up to support individual user communities, and an extra security function is needed for one of those communities, it's much easier to identify what documents need changing, in what way.

The following points in particular should be considered, and will be considered briefly in turn.

a) Each document should have someone (a post, not a person) clearly identified as responsible for keeping it up to date and reissuing as necessary;
b) Soft and hard copy of documents should be properly and accountably stored, much as one would look after source code;
c) There needs to be a way of registering that significant changes in system circumstances have, or will, occur;
d) Links with re-accreditation procedures have to be established.

<u>Maintenance and Re-issuing</u>

Whoever is assigned the responsibility for this need not do any word-smithing themselves. They are there primarily to ensure that it is done both accountably and well. The documents must remain fit for purpose. For example, an SP is the primary benchmark against which information security audits will take place. It is also the main source of information about pertinent threats, justifying the expense of counter-measures. If an audit reveals that the circumstances have changed, and that some

threats are no longer applicable, then unnecessary counter-measures might be continued. This means that unnecessary costs would be incurred by the organisation. The SP is no longer describing an effective security profile. And then of course, there's the possibility of new, unacknowledged, threats. So, the mechanism for maintaining and re-issuing security documents must be established. It doesn't really matter who gets this job, as long as it is a person able and willing to do it. One should, however, beware of assigning it to a person rather than to a post in the organisation. Sally in accounts might be the ideal person to look after the warehouse system SP because in her last post she did the business analysis for it, but she might leave and be succeeded by Fred who's straight out of college and doesn't know an SP from a doughnut.

Document Control

This principle is well established. If a document is likely to need maintenance, its 'source code' must be accessible, and controlled. This doesn't imply a huge bureaucracy; a simple locked box of floppy discs, in the care of the Head of Security's PA might be sufficient. Controls of this sort must be backed up by some way of readily distinguishing draft documents from ones which have been issued formally. A document's status must be obvious. Most organisations have this well under control, with long established formats and procedures.

Recognising The Need For Change

There are a number of ways in which the need for change might become obvious. A test run of the Business Continuity Plan might reveal that a key database cannot be readily recovered onto the standby platform. A security audit might reveal that a user security procedure has to be ignored if a particular telesales function is to be performed fast enough. A system manager may discover that loading a security-relevant operating system patch knocks out a key application. These things will happen - they are part of life. There must be a way of recognising and registering them when they occur. Once registered, someone has to have ownership of the problem, and for finding, if not a solution, at least a resolution. At its most basic, this means putting the incident reporting procedures into the user security guides, and making sure that exercises like contingency plan testing and security audits are properly documented, with a relevant readership responsible for acting upon what they read. Even the best documents rapidly decline in usefulness if there aren't appropriate organisational measures underpinning them.

Re-accreditation

This follows on naturally from the last point. Accreditation accepts the costs and residual risks of using IT resources in a particular way under particular circumstances. If the circumstances change, either the costs or the residual risks might become unacceptable. The supporting documents must therefore change to reflect accurately the new accreditation conditions. Sooner or later information security documents are going to be used as a prime source of information for important decisions. If they are out of date or inaccurate, the wrong decision may be made. The accreditor needs good documents, and good documents need the accreditor's imprimatur.

A Passing Thought

The risks may have been properly assessed. The counter-measures may be well chosen. The documents may have been carefully produced. But sometimes, ambiguities creep in - ones we don't ourselves see. Sometimes procedures don't work as well as we think they will. We should listen before we write, and then listen again afterwards, and make it clear not only that we are doing so, but also that we will take notice of what we hear. Don't be afraid to change something if it doesn't work, and to be seen to change it. Inflexibility is not strength.

Presentation

There are a lot of things one could say under this heading - and most of them have been said in the many stylistic guides available to the writer of technical and procedural documents. So I will confine myself to a very few points, expressed in terms of security documents. These are:

a) Document Breakdown
b) Medium
c) Review

Document Breakdown

I've already mentioned various flavours of security policy documents, and of user security guides. Which should you choose? A Network Security Policy or a Community Security Policy? To what level of detail should one go? There is no one right way of structuring security documents, and don't let anyone tell you that there is. There are efficient ways, and appropriate ways, and ways which are neither. What is appropriate for one situation might be inadequate, or completely over the top for another. Still, if judgement were not needed we could get the whole process automated, and let humans get on with more interesting things. Choose a document structure which avoids duplication, reflects organisational realities, allows you to target a clearly defined readership, and is readily maintainable. And it doesn't actually matter whether the document is called a Network Security Policy or a Community Security Policy. If the title is appropriate to the content, and the writers and readers know what is meant, enough has been done. Don't be afraid to be imaginative in how you organise and present information.

Medium

Again, don't be afraid to be imaginative. Is paper always the best medium? Would a user security guide be better on the corporate intranet? Should it be a document on its own, or should it be a section of the system's general user guide? Would some sort of Computer Aided Instruction package be appropriate instead of a paper document? The right solution is the one that works effectively and efficiently. The medium isn't always the message, but the choice of medium will always tell the reader something - even if it's not something you intended.

Review

There is no need to fly solo when producing security documents, especially ones which other people are going to have to use every day. The concept of independent review is well established and valuable. It need not be formal - not all situations merit that. If you are writing documents (in whatever medium) for operational use, get a reviewer from the operational area in question. It can be advantageous to ask someone not readily sympathetic to your point of view. This will get you brownie points for your confidence and openness, and should increase the rigour of the review (unless you've chosen a particularly Machiavellian individual). And it's not only software that can be beta-tested. Operational documents and procedures in particular can be amenable to this form of review. This can also increase user buy-in, especially if you listen and respond to reasonable observations.

Reprise

This is the repeat section. Everything here has been said in one way or another elsewhere in this

paper - thus ignoring the non-repetition point I have made several times. But judging from the many security documents I've read over the years (and one or two that I've written), the points are worth making again.

a) Information Security documents are written not just to be read, but to be used and to be understood.
b) Say only what is needed. Writing is not the human equivalent of a core dump.
c) Write in the language of the reader, not the writer. And the reader's language is often that of business, rather than of access control, authentication, object re-use, etc. etc.
d) Be imaginative.

Closing Comments

At the time of writing (late January 1998), I am in the process of completely rewriting the United Kingdom's Information Security Memorandum 5, which describes UK government policy on the compiling and documenting of information security information for civilian and military IT systems. By the time of the Conference, the new version should be in its beta-test phase. It will advocate the principles outlined in this paper. It will give examples of good practice, but will make the point strenuously that it is the local security and business authorities who are responsible for ensuring that their documents are fit for purpose. We in the United Kingdom Security Authorities are not going to sit at the centre and tell everyone what constitutes fit for purpose in everything from a Royal Navy artillery targeting system, to a stand-alone PC processing contract details, to a nationwide distributed tax system with thousands of users.

Two years ago in Baltimore, some of you may have attended the Panel Session on UK approaches to Risk Management in both government and industry. It will have been apparent that these two sectors are rapidly converging in their approaches to information security. The new Memorandum 5 will consolidate this philosophy by seeking compatibility with British Standard 7799 on information security management (details of which can be obtained from the United Kingdom's Department of Trade and Industry), and by reflecting best practice from both government and industry. In support of this, we hope to make the Memorandum publicly available. At root, the issues of confidentiality, integrity and availability are the same in both sectors. Government too seeks the efficient pursuit of legitimate business objectives, and that is what information security is about.

We anticipate providing Memorandum 5 not only in paper, but also in electronic form. At the time of writing this paper, we are looking at HTML, Windows Help format, and at availability using Web resources. We are trying to do as we preach.

To return to an opening metaphor: Scylla and Charybdis were monsters from Greek mythology who lived under rocks on opposite sides of the narrow Straits of Messina, between Sicily and mainland Italy. They snatched and consumed sailors from passing ships. We are doing our best to give sailors the charts and other information they need to pass by those straits in safety. But ultimately it's the helmsman who must steer the boat. Too much information or too little? We in the Security Authorities will give our clients good charts, but we'll leave the steering to them.


CESG

CESG

Communications-Electronics Security Group

Excellence in Infosec

CCSG

EFFECTIVE INFORMATON SECURITY DOCUMENTS

The British Approach

Excellence in Infosec

CESG

Michael E.J.Stubbings
Communications-Electronics Security Group
Room 2/0503
PO Box 144
Cheltenham
Gloucestershire
GL52 5UE
United Kingdom

Tel: +44-(0)1242-221491 ext 4035
Email: mike_stubbings@cesg.gov.uk

Excellence in Infosec

CCSG

OLD INFOSEC MEMORANDUM No 5

- Memo Title: System Security Policies
- Cradle to grave documents
- Mid-size office-based defence systems
- Confidentiality aspects only
- Presentation

CCSG

NEW POLICY PRINCIPLES

- For accreditation, not procurement or evaluation
- Local autonomy
- Quality criterion: fitness for purpose
- British Standard (BS) 7799
- Integrity and Availability
- Boundaries
- Improved presentation and distribution

CESG

OUTLINE OF NEW MEMO 5

See session handouts

CCSG

SUMMARY

- HMG Infosec interests are business driven
- One size does not fit all
- The right document is the one that works
- Boundaries
- Imagination