INFORMATION SECURITY IN A COMPLEX DEFENCE SYSTEM PROCUREMENT: A PERSONAL MANAGEMENT EXPERIENCE[1]

Wing Commander R J Kennett RAF* and Dr. M J Nash**

***Ministry of Defence**
Penderel House, High Holborn, London WC1V 7HX, United Kingdom

****Gamma Secure Systems Limited**
Diamond House, 149 Frimley Road, Camberley, Surrey, GU15 2PS, United Kingdom

ABSTRACT

This paper is based on the personal experience of the authors, and describes some of the real world management problems that they have encountered during the early development stages of a large and complex logistics IT system for the Royal Air Force. It covers some of the practical and pragmatic solutions that have been devised to ensure value for money and meet the user requirements, whilst ensuring that the necessary security is maintained.

INTRODUCTION

In 1986 it was decided that the four main elements of the UK Ministry of Defence (the Royal Navy, the Army, the Royal Air Force and the Ministry of Defence Procurement Executive) would undertake strategic Information Technology Studies. These would be conducted in the three main functional areas of logistics, personnel and command and management. The Royal Air Force started its logistics strategy study in 1988 and it was completed in 1989. The study had as its aim to define the IT strategy required to support the logistics objectives of the RAF into the 1990s and beyond. The principal objectives were to define the target IT systems required, specify a plan for migration from existing systems to the target systems, determine the organisation required to manage and control the migration, and specify the management activities required to implement the strategy.

The results of the study were that by initiating a 10 year programme of IT development costing about £500M (C$1,000M), the RAF would save in excess of £1000M (C$2,000M). This would provide the RAF Logistics community with a fully integrated IT system covering the Supply and Engineering organisation. It was also recognised that the system would need to process classified information and thus, security would need to be addressed from the outset.

Any computer system in the UK which is used to process classified information must be accredited. This is the formal confirmation by the Security Officer of the appropriate Governmental department (DSO) that the security requirements have been met and that use of the system in accordance with the System Security Policy (SSP) does not present an unacceptable risk to national security.

The SSP, and the Accreditation for live operation which is based upon it, take into account the overall security of the system. This is be achieved using a combination of technical and non-technical security measures, which may be interrelated. Where the SSP calls for technical security measures to be enforced by the system (as distinct from those enforced in the surrounding environment), the Accreditor may require certification by the UK Certification Body. Here, certification is a formal statement of the extent to which the security functions implemented in hardware, firmware and software meet the security requirements. In the UK, certification is based on the results of an

---

[1] PUBLISHED AT THE FIFTH ANNUAL CANADIAN COMPUTER SECURITY SYMPOSIUM, OTTAWA, CANADA, 19-21 MAY 1993. (pp. 59-69)

independent computer security evaluation, which is conducted by a Commercial Licenced Evaluation Facility according to standards and procedures mandated by the UK Government.

Historical studies into RAF logistics systems identified that in many areas the planning, management and control of logistics functions is manpower intensive and imprecise. There is a serious lack of information about logistics activities and their associated costs for use in policy formation and review. Existing logistics information systems have largely been designed to meet operational needs of discrete groups of users and were not designed to share common data or provide aggregated management information. The major RAF central logistics IT systems currently employ ageing technology and use inconsistent technical and data standards. More importantly, they do not meet the users' current needs. Overall, existing IT systems do not provide a sound foundation for future development.

The Royal Air Force is committed to achieving year-on-year savings in running costs which are likely to remain under continuing pressure for the foreseeable future. With the increased emphasis on financial restraint, operational commitments can only be met through substantial and sustained improvements in support efficiency. Logistics support costs represent a significant part of the total Air Force funding and therefore offer a major opportunity for savings.

Recent investigations have included extensive analysis of the RAF logistics tasks from a business standpoint. This analysis reveals the difficulties that would be encountered if RAF staffs were forced to achieve their logistics mission, given the current budget constraints, if they were required to use existing support facilities.

IT SECURITY STAFFING

A Directorate of Logistics Information Systems(RAF) was set up in 1989 to manage the development of the Logistics Information Technology System (LITS) and to continue to manage the current RAF logistics IT systems until they were subsumed by LITS. From the beginning, IT security was seen as a major risk to the programme which would need to be managed on a full time basis: this was a new idea for the RAF. A full time post was established at squadron leader (major) level to take on the responsibility for this area.

In the light of experience, a year into the project, and with the knowledge of future requirements, it was seen that the responsibilities of the post were greater than originally envisaged and it was deemed essential to raise the level of the post from a squadron leader to a wing commander (lieutenant colonel). This decision has proved to have been correct and it was made just in time.

The wing commander is responsible for setting the IT Security Policy for the LITS programme, within the general guidelines set out by the RAF security authorities. It was decided that the incumbent for this post should have a RAF logistics background because at the project development level it would be important to understand the implications of the policy being developed. IT experience and appropriate IT security training was also thought to be essential. All of these criteria have been fully justified. This post is supported at the strategic programme level, and for specific security studies, by experienced IT security consultants contracted from industry. This has resulted in a strong IT Security Policy Branch, able to maintain effective control over IT security within the Programme.

LITS CONTRACT STRATEGY

One very important aspect that strongly influenced our approach to IT security for the LITS was the contract strategy for the procurement. It was decided early in the Programme to split the work into three major tranches. Each tranche would cover specific application areas. Furthermore, each tranche would also be split into two parts for contract purposes, a full study contract, to undertake the requirements definition and analysis, and a development and implementation contract. Moreover, the two contracts would be mutually exclusive, and any contractor winning the full study would not be allowed to compete for the development contract. The winning contractor for the development of the first Tranche would also become the Primary System Integrator (PSI) and thus be responsible for running the development of the other two tranches.

SSADM

Structured System Analysis and Development Methodology (SSADM) is the UK Government's preferred systems study method and it was decided to impose it on the LITS programme. SSADM is a 'waterfall' based methodology which involves both functional and data analysis. It can be simplistically split into the following 6 sequential stages:

a. Investigation of the Current Environment
b. Business System Options
c. Requirement Analysis
d. Technical System Options
e. Logical Design
f. Physical Design

SSADM is a comprehensive methodology with well defined outputs and data flows. Unfortunately, it does not address IT security requirements. Standard security documentation for systems processing classified information are set out in a number of guidance memoranda issued by the UK's Communications-Electronics Security Group (CESG), the UK national authority for INFOSEC. These include a number of security policy documents at differing levels of detail. Security deliverables need to be specifically addressed in the life-cycle of a secure system, in addition to the standard SSADM deliverables. We could not find anybody who would admit to having tackled this problem before, even though we understood that it was a known problem! Our first approach was to list the security products we needed from the study, starting from WHAT we thought we needed at the end, and then we decided WHEN we would want them produced within the SSADM framework.

In particular, for LITS we had to take into account the change of contractors at the end of SSADM stage 3, the Requirement Analysis stage. The output from the study contract would be used to support the Operational Requirement for a development contractor. The responses to this Operational Requirement from Industry would, in essence, represent stage 4 of SSADM, that is providing us with a set of Technical Systems Options from which we will choose one. The development contractor will still be required to complete any remaining analysis for stage 4 and the work of stages 5 and 6. This caused some problems because the change of contractors at this point meant that we would be taking partially completed security documents and passing them to somebody else to first comply with and then to complete them. Furthermore, the deliverables from the Full Study would be used for the contractual negotiations for the design and development stages. This resulted in us having to slightly modify our original proposed list of deliverables. Furthermore, we had to ensure that the Full Study Contractor was committed to justifying the statements being made in the security deliverables and the direction in which we would be pointed, especially in respect of the security policies. Our modifications resulted in the following deliverables list for SSADM stages 1 to 3:

<u>Stage 1 - Investigation of Current Environment.</u>

a. Security threat assessment.
b. Description of current security facilities.
c. Statement of current system availability and integrity .
d. Requirements catalogue entries for security (including integrity and availability).
e. Outline System Security Policy.

<u>Stage 2 - Business System Options.</u>

a. Security analysis of each business option.
b. Security architecture options report.
c. Definition of the selected security architecture.
d. Generic elements of the System Security Policy including interfaces to other systems.

<u>Stage 3 - Definition of Requirements.</u>

a. Draft System Security Policy.
b. System Electronic Information Security Policy input covering only generic elements for authentication, access, audit and accountability.
c. Draft ITSEC Security Target, including a semiformal specification of security functions and identification of the underlying Security Policy Model for those

components where the identified ITSEC evaluation level is E4 or higher (formal specification at E6).

d. Security contribution to other aspects of the Operational Requirement documentation.
e. The identification of any security relevant contractual issues relating to the remaining SSADM stages, including security cost estimates and security evaluation strategy.
f. Final statement of integrity and availability requirement.

Having decided on the deliverables for the first three stages we then derived the following list of deliverables for the development phases.

Stage 5 - Logical Design.

a. Agreed System Security Policy.
b. Agreed System Electronic Information Security Policy.
c. Any changes to the ITSEC Security Target following from the PSI's technical solution.
d. Security Policy Model (only for any system components eg. Guards requiring assurance at ITSEC E4 level or higher). (May well be a null or COTS item).
e. Evaluation Contract. (PSI must contract for evaluation with an approved ITSEF.)
f. Draft Secure Operating Procedures. (First version of user and Security Officer instructions.)

Stage 6 - Physical Design.

(Some internal deliverables to the ITSEF).

As SSADM stops at the end of design, we needed to complete the development life-cycle for security products and the following additional deliverables were identified:

Implementation. Installation. Acceptance and Integration

a. Final System Security Policies. (PSI is responsible for taking the agreed documents from SSADM Stage 5, and modifying them to correspond to the system as finally accepted by the user and security accreditor.)
b. Approved Secure Operating Procedures. (Based on draft document from SSADM Stage 5, modified in light of actual operational structure and difficulties identified during acceptance.)
c. Evaluation certificates to support accreditation process.

We are currently at SSADM Stage 3 and our experiences so far are that we were not far out in what we would have asked for if we had known then what we know now. However, in the light of our experience we would have changed the following:

a. We would have contracted for a more explicit input to the Operational Requirement for the PSI contract from the Full Study Contractor.
b. We now realise that it is not possible to adequately detail the security architecture at SSADM stages 2 or 3 of SSADM. This is because insufficient technical information is available before SSADM stage 4 to assess the viability of potential security architectures.

PRINCE

PRINCE stands for Projects in a Controlled Environment and it is the UK Government's preferred methodology for managing projects. It consists of 5 major components which define the structure of the control for a project and which are applied to the stages within a project, as follows:

a.	Organisation	-	Project Board, Project Manager, Stage Manager and Project Assurance Team
b.	Plans	-	Technical, Resources, Quality and Exceptions
c.	Controls	-	Management and Technical
d.	Products	-	Management and Technical
e.	Activities	-	Management and Technical

Again, we were faced with a methodology which did not address the needs of security and we had to start from scratch. However, CESG provided guidance on this subject in the form of a formal memorandum. Unfortunately, this could not be directly mapped onto the project management organisation being introduced for the LITS programme. LITS was to follow the principles of PRINCE for the RAF management team, but we did not want to compel the contractor to use the same methodology as long as we could interface our PRINCE organisation and requirements. CESG's proposals were mainly two fold, firstly the DSO should sit on the PRINCE Project Management Board, and secondly the Project Assurance Team (PAT) should include a Security Assurance Coordinator (SAC). The role of the PAT is to review all deliverables at each stage before their acceptance by the Project Management Board.

We realised that the role of the SAC within the PAT proposed by the CESG guidelines would be a full time task on a project the size of LITS. Yet, because it was the intention to devolve as much responsibility and work as possible to the Contractor, the RAF PAT would only undertake audit verification and validation, that is only a percentage check of the contractors deliverables. Thus, we insisted that the contractors team included a security advisor (SA) with the prime responsibility of monitoring and reporting on all security matters relating to the Tranche, in other words performing most of the role of a SAC. Over and above this the LITS IT Security Policy Branch would maintain an additional watching brief on policy issues and liaise with the relevant security authorities. In addition a strategic security working group would be set up to keep overall control of the programme.

The main responsibilities with which we tasked the contractors SA are as follows:

a. Resolving day-to-day security issues in conjunction with the Tranche Security Working Group (TSWG).
b. Advising the RAF's PAT and the TSWG on security considerations arising from the work of the project teams, including identifying any non-IT security measures that may be required when in service.
c. Reviewing all work being undertaken for the Tranche to identify any inconsistencies with strategic security considerations or with the Tranche security studies.
d. Providing electronic security advice to the TSWG and the Tranche project teams.
e. Channelling advice from the security authorities to the TSWG and the Tranche project teams.
f. Making documentation available to any independent evaluation agency.
g. Arranging the attendance of members at the TSWG appropriate to the subjects under discussion.
h. Attending meetings of the LITS Strategic Security Working Group as required by the LITS IT Security Policy Branch.

Our experiences with our revised PRINCE organisation so far, are similar to those that we had with SSADM. It has been very successful. The appointment of a SA has been invaluable to both the FSC and the RAF. We have experienced some minor problems with the procedure for reviewing documents, which now involves a number of separate parties that vary according to PRINCE review type and we have had to make minor changes to the procedures that we believe will prove successful. There was some resistance with getting an IT security representative onto the project board but this has been overcome.

LESSONS LEARNED

Firstly, if security is important to any project then it is important to have somebody specifically responsible for IT security. Whether this is a full time task or part time will depend on the size of the project. Furthermore, IT security is not a dead-end, so the person employed on it must be interested in the subject. It is also important that the person is at the right level of management and to ensure that your organisation provides that person with support at the highest level of project management.

Try to anticipate problems before they occur. Although this sounds like crystal ball gazing, it is the mark of good project management. Anybody involved with IT development knows roughly the project goals and the general route to reach them, and so it is possible to anticipate most problems. Also, keep in touch with everybody involved with the project. We have recently realised that we were not seeing the contractor's security team to routinely exchange information and ideas, so we now hold regular

weekly meetings, irrespective of meetings called to discuss specific points. So do not be frightened to change direction occasionally.

If you have a contract with a developer or study contractor make sure you include IT security as part of the contract and state precisely what you want the contractor to do. One of the UK IT Security Evaluation Facilities managers told me that you only get the same level of security from a contractor as the level of importance that you give to IT security in the contractual documents. Make sure that the contactor is aware of what deliverables you want from the contract and check how he is to achieve them.

It is important to recognise policy problems which must be resolved at a policy level. We feel that if we had blindly followed the generic thinking for controlling IT security for LITS within the PRINCE framework then we would have quickly overloaded the management system.

Finally, we have found that the development of good relationships with all concerned with the project and other related organisations, including the security authorities, has helped us enormously. I am sure that it has allowed us to resolve problems before they grew out of all proportion, and for everybody to be flexible within the terms of reference.